

## Chapter 11

# Keeping DR Plans and Staff Current

### *In This Chapter*

- ▶ Understanding how business changes influence DR planning
- ▶ Working disaster recovery into key business processes
- ▶ Outlining disaster recovery requirements and standards
- ▶ Looking into a DR case study
- ▶ Managing disaster recovery documents
- ▶ Keeping response teams prepared

**C**hange is a constant force in organizations of all shapes and sizes. Updates in technology, modifications to business processes, and other changes prompt you to revisit and revise your DR documents, including your Business Impact Analysis (BIA) and disaster recovery procedures. This chapter can help you understand the types of changes you need to make to your disaster response procedures and plans when changes in the business occur.

Speaking of changes, personnel changes often happen. People come, people go, and people move around on the *org chart* (who reports to whom). These new people in new roles require training and retraining to keep teams and departments ready if a disaster occurs.

## *Understanding the Impact of Changes on DR Plans*

By their nature, businesses are undergoing continuous metamorphoses. Businesses change their business models, org charts, product and feature sets, and SLAs (Service Level Agreements) as frequently as you change your underwear.

## 242 Part III: Managing Recovery Plans

In the following sections, I discuss the types of changes that occur in businesses and the impact those changes have on disaster recovery plans. I group these changes into five categories:

- ✓ **Technology changes:** Upgrades or changes in software, hardware, and other technologies.
- ✓ **Business changes:** Changes in processes, mergers and acquisitions, and relocation.
- ✓ **Personnel changes:** Changes to the org chart, attrition, changes in department and individual responsibilities, and so on.
- ✓ **Market changes:** Over time, you change the way you make and price products or services, and your consumers change how they consume and think of those products or services.
- ✓ **External changes:** Other events that occur outside of the business itself that change your business's risks in some way.

If you don't think the preceding list was detailed enough, the following sections put each of these areas under a powerful electron microscope. Remember not to squint too long, or your eyes will hurt.

### *Technology changes*

Paper tape gives way to punch cards, which reel-to-reel magtape displaces, which yields to tape cartridges, and then optical media . . . technology just marches on and on. Every step of the way, technology upgrades require revisions to disaster recovery procedures. The following sections give you some examples of technology changes.

#### *Upgrades to IT systems*

Changes at every layer in the stack (application, database, operating system, and network) can mean you need to change DR procedure documents. Some examples of such changes include

- ✓ **Network devices and software:** New routers, firewalls, load balancers, and even just software upgrades.
- ✓ **Server, storage, and tape library hardware:** With new hardware, the buttons are always in new places and the labels look a little different. Are your DR procedures still accurate?
- ✓ **Operating system (OS) change-outs or upgrades:** If you change from one OS to another, you need to rewrite your DR procedures. But even upgrades may require edits to procedures if command options or other OS procedures have changed.

- ✓ **Changes or upgrades in higher layers:** Such as in the database management system (DBMS) or application server. It seems like change is the only constant, which means you need to make changes to your disaster recovery procedures. Will it ever end?
- ✓ **Media changes:** Whenever backup media, archival media, or software release media change, you may also need to change the procedures for recovering systems.

### ***Introduction of new IT technologies***

New technologies are rolling in all the time — from USB tokens to optical media to biometrics. Whenever you incorporate any of these new technologies into an application or infrastructure, you probably need to change your recovery documents.

## ***Business changes***

Senior managers and executives in organizations sometimes make decisions that have a moderate-to-profound impact on the entire business. These range from changes in existing business processes to more significant changes such as mergers and acquisitions, outsourcing and insourcing, and changing business locations. All of these changes require you to review DR documents on some level to make sure they're still relevant and accurate.

### ***Business process changes***

Organizations change their processes with frightening regularity. The trouble is, some businesses make these changes subconsciously — meaning the businesses don't plan the changes, they happen spontaneously and aren't well documented or communicated. On the other hand, many organizations have a process for changing processes, so hopefully the *process-change process* (the process for changing processes) includes a step to review and edit disaster recovery procedures.

### ***Mergers and acquisitions***

A *merger* (when two businesses become one) or an *acquisition* (when one business purchases another) can upset the boat like few other changes can. When a merger or acquisition occurs in an organization, priorities can suddenly change or go sideways. The ramifications include

- ✓ Highly critical business processes may become less critical.
- ✓ Business processes previously considered not critical may suddenly become critical.
- ✓ Processes may alter.

## 244 Part III: Managing Recovery Plans

- ✓ Processes often combine.
- ✓ Sometimes, your business scraps a process in favor of a similar process in the acquiring (or acquired) business.
- ✓ A merger or acquisition wreaks havoc on org charts. (I discuss these types of changes in detail in the section “Personnel changes,” later in this chapter.)
- ✓ Business or personnel often relocate.
- ✓ IT applications face big changes — winning applications survive and losers get scrapped.
- ✓ The new organization may place more value on disaster recovery, changing all the results in the Business Impact Analysis (BIA).



An organization that undergoes a merger or acquisition should consider revisiting its BIA to reevaluate the MTD (Maximum Tolerable Downtime), RTO (Recovery Time Objective), and RPO (Recovery Point Objective) figures relating to post-merger/acquisition processes. You may have different priorities and thresholds in the new organization. Newly placed executive management may also have new opinions on the importance of disaster recovery.

### *Changes in business locations*

Businesses that change their business locations may have a few — or many — changes that require a review of disaster recovery procedures. If a business is moving a short distance, make changes to the procedures just to reflect changes in the physical environment. But if your business moves a significant distance, you may need to change some of its suppliers (such as off-site media storage), as well as some of its technical architecture. (Moving gives you a good excuse to make changes to processes, which translates into changes in recovery procedures.)

### *Outsourcing and insourcing*

When a part of an organization transitions from insourced functions to outsourced functions (or vice versa), you must change any DR plans related to the part of the organization that was insourced or outsourced. Here are some examples of outsourcing changes that require consideration:

- ✓ **Newly outsourced function:** If you have a DR plan for this function, the business needs to coordinate the development of recovery procedures with the new service provider.
- ✓ **Newly insourced function:** If you need a DR plan for an insourced function, develop new recovery procedures and train staff in the organization on those procedures.

- ✓ **Changes in dependencies:** Sometimes, a process's big picture changes in a way that alters dependencies on internal or external resources. For instance, if the DR plan for a process depends on the services provided by a department that's now outsourced (or insourced), you need to change the recovery plans to accommodate the changes introduced by the outsourcing or insourcing.

I don't have any magic formulas for how you need to change DR plans when insourcing or outsourcing occurs. You need to carefully analyze all affected business process and recovery plans, and make adjustments that permit the DR plans to work, even after the business makes the insourcing or outsourcing changes.



If your business switches an outsourcing partner, revisit any DR plans associated with the process(es) performed by that partner to make sure the services provided by the new partner are still compatible with existing DR plans.

## *Personnel changes*

Organizations fire, hire, and rearrange their workforces on an almost daily basis. It's no wonder that companies don't publish their org charts as often as they used to: By the time the chart's printed, it requires another update. These types of changes have a bearing on DR planning, as I discuss in the following sections.

### *Organization chart changes*

Even if no one leaves your organization and you don't bring anyone in, just changing the command and control structure may have some — perhaps a significant — impact on disaster recovery plans. Here are some examples (as told by a department manager):

- ✓ **That's not my department's job any more.** The experts who wrote disaster recovery plans and manned the recovery teams may suddenly be unavailable. You need to train new staff members, and you may have to edit the DR procedures.
- ✓ **They took my staff away.** See the preceding bullet.
- ✓ **That's my function now.** The opposite of the preceding bullets. A manager is newly responsible for a function covered by the DR plan. Your staff may need training, at least, and you may need to change your DR procedures to accommodate the staffing changes and possible process changes that result from the change in responsibility.

## 246 Part III: Managing Recovery Plans

- ✓ **That dependent function is now out of my control.** Processes always have dependencies. A team that previously handled the DR plan for a business process is now split up. Can the former team still function as a team? Management needs to discuss these changes and what you need to change (if anything) in DR plans and procedures.

At the risk of sounding preachy, I want to say to managers at every level when facing the challenges of the reorganization of the month: Be responsible and figure it out. No one said it would be easy.

### *Relocation of key employees*

*Relocation* involves an employee moving to a different town or city. To be more specific, one or more key personnel whom you depend on in a disaster situation now lives 20, 50, or 100 miles away. In a disaster, such personnel may not be able to travel this distance to be on-hand as part of a recovery team.

In the best-case scenario, you simply need to train personnel who live closer to business locations. In the worst case, you don't have any suitable trainees who live close enough to be there when a disaster strikes — a problem without an easy solution. Maybe you need to offer that employee who moved away more money to live closer, or perhaps you can hire another expert who lives close by (and hope he or she doesn't move away). Those pesky employees, always making life decisions that don't put work ahead of other considerations! (I'm kidding, of course — your employees are your most valuable resources.)

### *Telework*

Technology and changing business attitudes have led to people living further and further away from their places of work, and many work permanently from home. This shift especially applies to information workers who are technically savvy and can use technology effectively from any location, whether in the office or hundreds of miles away.

Having access to the wider community of gifted workers can make finding new talent easier, and you can hire that talent without requiring that they live within a short drive of your business location. But the telework equation can go awry during a disaster. For many reasons, you may need those workers all on-site when disaster strikes — but if half of them live out of town, fat chance of that!

This situation does have an up side: If a regional disaster strikes your business location, many of your local employees may be wrapped up in the disaster, caring for family members or just trying to keep their belongings safe. But your out-of-town teleworkers may be unaffected by the disaster (because they live far enough away, out of the disaster zone), so they don't have any of the disaster-related distractions keeping them from working. As long as your

business has enough infrastructure still working (such as VPN/remote access and telecommunications), your teleworkers can keep on working over the wire. They can carry out their usual duties, and perhaps they can even perform most or all of the procedures in a disaster recovery plan.

### ***Staff attrition***

It's a fact of life — people come and people go. You need to periodically train new personnel on disaster recovery procedures. Attrition can cause real problems if you no longer have any subject matter experts who can perform critical recovery functions. Smaller organizations that have only one expert in several subject areas can really suffer from such an extended absence. For this reason (and many other reasons), make your disaster recovery procedures highly detailed so non-experts can carry them out without fear of making deadly assumptions or mistakes.

## ***Market changes***

Whatever your business does, the market is always changing. Products and services grow and change, and the dynamics of the production of your company's goods and services never stand still. Sometimes, these changes are profound enough that your BIA results change, which impacts MTDs, RTOs, and RPOs, all of which can change your recovery procedures. The following sections look at some of these factors.

### ***New production or delivery methodologies***

The ways in which businesses such as yours develop and deliver goods and services change slowly over time, and sometimes bigger, more disruptive changes radically influence how you do what you do. Here are some examples:

- ✓ **Increased outsourcing:** As a flanking move, one competitor outsources a part of its operation to save costs, and other competitors follow suit to retain competitive parity. Outsourcing critical functions has a profound effect on DR plans and who carries them out.
- ✓ **More efficient production or delivery:** Innovation sometimes introduces new methods that make the production or delivery of products and services more efficient. Innovation changes the entire cost (and, often, pricing) structure for an organization, which in turn affects all of the MTD, RTO, and RPO formulas, affecting your overall BIA results.

These kinds of changes sometimes occur slowly, and at other times, quickly. Sometimes, you don't recognize them until well after the fact. Revisit the BIA every year or two, or more often in rapidly changing industries, just to make sure that the numbers still support the level of DR planning and testing activities currently taking place.

## 248 Part III: Managing Recovery Plans

### ***New competitors and changes in market share***

Every time a competitor enters or leaves a market, or when any given organization has a significant change in market share, the economics of production and delivery change. These changes can greatly influence MTD, RTO, RPO, and BIA formulas and results.

### ***Supply-chain changes***

In complex business ecosystems, changes such as innovations, big price swings, or sea changes among partners or suppliers can profoundly influence your own business operations. For example, consider a big rise in energy costs due to hurricanes disrupting oil production and the ripple effect that those price increases have on many industries.

Sometimes, this influence is big enough to force you to revisit your BIA, MTD, RTO, and RPO figures. Sometimes, the changes increase the need for DR response capabilities, but at other times, those changes decrease the pressure to respond quickly to a disaster.

## ***External changes***

An entire class of changes can take place outside of the business. These kinds of changes can influence risk (up or down) or impact recovery procedures. The following sections by no means give you a complete list; other events and situations can also affect your DR plans and procedures.

### ***Nearby construction***

Major construction projects that take place near your business premises may change your business's risks in some way. For instance, if a factory is built nearby that handles hazardous materials, the chances that you may need to evacuate your own premises increases somewhat. If a new freeway is constructed near your business, you may have better transportation options, which may improve regional transportation capabilities during a disaster. If a facility that provides or promotes controversial services is built next door, you have an increased chance of nearby protests or civil unrest. Or, if that gasoline pipeline that passes your business is aging, a gas pipeline rupture and fire may soon happen too close to your business. Changes in nearby businesses may also affect crime rates.

### ***Utilities changes***

Changes in power grids, telecommunications, and natural gas delivery affect your organization. Over time, electric power and telecommunications may become less effective because of aging facilities, resulting in more frequent or lengthier outages.



### ***Regulation***

It may take just one significant event to motivate the government to pass a new law. Sometimes, these regulations indirectly influence your DR plan by changing the fundamental economics of businesses in a particular location or sector. These changes can, in turn, influence your DR plans.

### ***Political events***

Changes in local, regional, and national government leadership sometimes result in big changes in certain industries — some favorable and some not so favorable. The fortunes of businesses large and small sometimes hinge on elections and other political events. If I haven't struck a chord with you, perhaps your organization is immune to the political winds that blow. But will it always be?

### ***Disasters***

Besides the obvious and immediate effects on a business, disasters sometimes have longer-term effects in a region. Often, local or regional government invests in infrastructure that can better withstand future disasters. Sometimes, the changes that take place affect building codes and may even require your business to retrofit your safety systems.

Some of these changes can help a business by reducing the impact of future disasters, but they can also raise costs directly or indirectly.

## ***Changes — some final words***

Some changes, such as technology changes, require only changes in disaster recovery procedures. Other changes, such as mergers and acquisitions, are so profound that you must redo the entire Business Impact Analysis (BIA) to recalibrate business priorities.



I don't have a magic way to classify changes as big or small. But if your organization has instituted a DR plan steering committee, that group should make those judgments if and when needed. When the events discussed in this section occur, whoever in the organization has overall management responsibility for DR planning needs to enact reviews of BIAs, RTOs, RPOs, MTDs, and recovery procedures. These documents and figures probably won't get up on their own and begin updating themselves. Someone high up in the organization's management structure must have his or her finger on the pulse of the entire organization so the events discussed here can precipitate proper reviews in disaster planning and response.

## 250 Part III: Managing Recovery Plans

### *Incorporating DR into Business Lifecycle Processes*

Organizations use processes as a part of introducing changes into their processes. Yes, that was a recursive statement — using processes to change processes. More mature organizations use a specific set of procedures when making changes to its business processes.

But only some businesses consciously realize that they actually use a process to modify their processes. Many organizations change their processes spontaneously and without a lot of planning or analysis.

Regardless of whether your organization effectively manages its processes, consider the impact of every process change on your DR plan, and vice versa.

The following sections discuss three areas of lifecycle processes:

- ✓ Systems and services acquisition
- ✓ Systems development
- ✓ Business process engineering

When you make disaster recovery planning a part of these key processes, you make the organization naturally more proactive by including disaster recovery planning as a part of doing business, rather than as an add-on.

### *Systems and services acquisition*

When an organization considers the acquisition of a new IT application or service provider, you need to devote a lot of thought and planning to ensure that the organization chooses the right application or service. Make sure the application or service has the right features and configurations that can meet your organization's needs.



Keep this key point in mind, particularly during the decision-making process for a new application or service: The application or service needs to support the needs of the business process(es) that it supports, not the other way around. Often, an organization makes a poor choice by selecting an application or service that doesn't meet the needs of the business; as a result, the business has to change its processes — sometimes in significant ways — so it can use the application or service.

DR planning is, first and foremost, a business activity in which business decision makers identify the most important business processes and how quickly the business must recover those processes if a disaster interrupts them. After you identify these key items (primarily your Recovery Time Objectives, or RTOs), the business needs to make all necessary changes to processes and IT systems to support those objectives.

Similarly, when the organization considers purchasing an application or service that supports a critical process, make sure the application or service meets established recovery needs. If you apply this principle to the systems and services acquisition process, whenever you acquire a new application or external service, you're on the right path to ensure that you can achieve your established DR objectives, particularly Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Meet these objectives in the systems and services acquisition process by incorporating your DR requirements into the complete set of requirements that you submit to each potential vendor. Then, when the vendors respond to each requirement, you know which vendors are more likely to deliver what you need. I discuss the development of requirements and standards in the section "Establishing DR Requirements and Standards," later in this chapter.

## *Systems development*

Although the trend for software and systems development has leaned heavily towards acquiring applications, many organizations still opt to build some business applications themselves. Also, many organizations still use applications that they developed in the past (as long as a decade or more ago).

Organizations that purchase COTS (common off-the-shelf) applications still need to develop custom software so these applications can communicate with each other. Many organizations develop customizations for COTS applications so they can get needed custom reports or analytical databases that the applications themselves don't provide.

Whenever your organization embarks on new software development — whether for a complete application, or for customization or integration purposes — you need to make many decisions so the resulting software meets the organization's needs. Those needs include hardware and software standards, security and privacy, and disaster recovery.

Often, DR standards are manifested through standards for hardware, software, database, and application. This helps to ensure that any new applications run on systems for which the organization has already developed

## 252 Part III: Managing Recovery Plans

resilient architectures and recovery processes. For instance, if an organization has developed product standards such as Sun, Solaris, and Oracle for applications that require DR capabilities, the organization can more easily recover any additional applications, customizations, or integrations that also run on Sun, Solaris, and Oracle by using existing DR plans and procedures.

I discuss the development of specific requirements and standards in the section “Establishing DR Requirements and Standards,” later in this chapter.

### *Business process engineering*

Whether they use a formal lifecycle and methodology, or make spontaneous changes, organizations exercise *some* level of discipline in their practices of business process engineering (BPE). I’ve been in organizations at both ends (and in the middle) of the discipline-and-formality spectrum. Generally speaking, organizations that are newer or smaller tend to make process changes more spontaneously, without fully considering the consequences of the changes that they make. Probably the only advantage of living on the low end of the process maturity spectrum is that you can make changes quickly — even instantly! But, oftentimes, those changes have unintended and unwanted consequences that you discover later on.

Towards the formal and disciplined end of the spectrum, organizations spend more time analyzing, planning, and designing their business processes. Organizations that spend more time planning tend to have processes that better meet their needs. The downside to this level of discipline is that it takes more time to make changes in business processes. Some organizations can spend so much time analyzing changes that they never seem to actually make any changes. I like to call this phenomenon *analysis paralysis*.



Business process engineering is similar to software development: Done right, both have lifecycle processes that include concept, requirements, design, testing, implementation, and maintenance.

I emphasize the requirements part of business process engineering in this section. Simply put, when you develop requirements, you first need to write down all the necessary characteristics of a business process before you design and implement the process. Or, if you have an existing business process that needs changes, you still apply the requirements, making sure that changes still support those requirements.

Any time you develop or modify business processes, you must carefully analyze the consequences of the new or changed process. Business processes need to support business policies about security, privacy, and disaster recovery. Establish new and existing processes in such a way that you can recover and restart them during a disaster, possibly working with only inexperienced

personnel. Thoroughly document the processes themselves, as well as all the procedures and tasks in them, and include recordkeeping tasks.

## *Establishing DR Requirements and Standards*

Creating a library of formal requirements for IT development and procurement projects can really drive consistency into an organization's technical environments. Companies often develop such requirements in several categories, including the following:

- ✓ **Hardware:** Using computing hardware from as few vendors as possible reduces support costs.
- ✓ **Operating system (OS):** Basing everything on a common OS standard permits an organization to support more systems with fewer IT support staff.
- ✓ **Database:** Common database standards permit an organization to manage all of its corporate data as a more cohesive whole, not as separate, disconnected islands.
- ✓ **Application services:** Centrally managing functions such as authentication, messaging, and audit logging helps to streamline application management.
- ✓ **Network protocols:** Common routing, messaging, and management protocols simplify network architecture and management.
- ✓ **Service layer:** A distributed computing service layer, such as Service-Oriented Architecture (SOA), facilitates integration between applications.
- ✓ **Application components:** Common environments based on Rich Internet Application (RIA) technologies, such as AJAX, Adobe Flex, and Silverlight, can improve the user experience by making the application more visually appealing or easier to use.

And, starting in recent years, organizations are developing requirements and standards in two new areas:

- ✓ **Security:** Common security protocols, programs, and devices make protection and security management simpler than if different parts of an enterprise use disparate features and products.
- ✓ **Privacy:** Common means and methodologies within applications, databases, and operating systems for protecting employee and customer private information.

## 254 Part III: Managing Recovery Plans

Organizations that realize the need for consistency in their environments for disaster recovery purposes can add a new category of requirements and standards:

- ✓ **Disaster recovery:** DR requirements and standards should include the selection of certain brands and technologies for new IT systems. The organization can then easily incorporate these new environments into existing DR plans without having to develop new procedure sets for each related technology.

Requirements and standards should lower support costs by driving the organization toward a more consistent environment, in which IT systems and applications use common standards, protocols, and technologies. This sameness provides a lower TCO (total cost of operations), making it easier for the organization to bring DR capabilities to more applications.

Without common standards and requirements, an organization's IT environment would resemble a computer museum that has one of everything. You'd need complete and separate sets of skills, procedures, DR plans, and support contracts for each system. I don't know many organizations that have that much money to spend on their systems.

### *A Multi-Tiered DR Standard Case Study*

In this section, I describe a moderately complex DR standard that a hypothetical organization, a relatively large enterprise that has a multitude of IT systems and a mature DR plan, develops. In honor of one of my favorite cartoon characters, I call this organization Acme Enterprises — or Acme, for short.

Acme has many dozens of IT applications that support its various critical business operations. Acme has performed many Business Impact Analyses and has developed several DR architectures over the years.

Acme settled on three sets of technology standards that it aligns with its RTO and RPO (Recovery Time Objective and Recovery Point Objective) groupings. Acme establishes its standards as follows:

- ✓ **Tier 1 DR standard:** The highest resilience that provides the fastest recovery time, almost immediate
- ✓ **Tier 2 DR standard:** Provides recovery time measured in hours
- ✓ **Tier 3 DR standard:** Provides recovery time measured in days

The three standards in the preceding list align with the three levels of recovery requirements that support virtually all business functions that require DR support.

Table 11-1 describes the three DR standards established by Acme in more detail.

<b>Table 11-1 Acme Enterprises Tiered DR Standards</b>			
<b><i>Specification</i></b>	<b><i>Tier 1 DR Standard</i></b>	<b><i>Tier 2 DR Standard</i></b>	<b><i>Tier 3 DR Standard</i></b>
The RTO (Recovery Time Objective)	3 minutes	8 hours	5 business days
The RPO (Recovery Point Objective)	1 minute	15 minutes	8 hours
Hardware manufactured by	Sun (servers) and Hitachi (Storage Area Network, or SAN)	Sun (servers) and Hitachi (SAN)	Sun or HP
Operating system	Solaris	Solaris	Linux
Database management system	Oracle	Oracle	MySQL
Web server	BEA	BEA or Apache	Apache
Clustering system	Solaris World-Wide Cluster	Solaris Metro or World-Wide Cluster	None
Data recovery	From mirror	From replicated data or backup tapes	From backup tapes
Testing requirements	Paper testing (whenever documentation is updated) and cutover testing (monthly)	Paper testing (whenever documentation is updated) and cutover testing (monthly)	Paper testing (quarterly), walkthrough testing (quarterly or after any major upgrade), cutover testing (annually)

Business requirements drive Acme's DR standards, specifically its RTO and RPO, not the other way around (some organizations fall into the trap of letting their technology and DR capabilities define business requirements).

## 256 Part III: Managing Recovery Plans

Systems that meet Tier 1 SR standards support Acme's most critical business processes. Acme has written a common set of DR procedures for Tier 1 systems; those procedures for recovering servers and data are virtually identical for all Tier 1 applications.

Similarly, systems that meet either Tier 2 or Tier 3 standards support Acme's important (but not critical) business processes. And like Tier 1, the recovery procedures for Tier 2 are practically identical to each other, as are the Tier 3 recovery procedures. In fact, the only variants in the recovery procedures within any of the three tiers are those steps specific to individual applications. The recovery procedures within each tier at the hardware, operating system, and database management layers are identical.

Acme developed a three-tier DR standard, instead of using just one standard (the Tier 1 standard) and making all systems that need disaster recovery conform to it, mainly because of cost. Building Tier 1 systems costs more than Tier 2 or Tier 3 systems because Tier 1 systems include clustering and mirroring components (which add costs). Systems that you can recover in days rather than minutes don't need to have the same expensive components that Tier 1 systems need to produce their near-real-time recovery. Acme has a lot of applications that require varying levels of recoverability, and it made sense to stratify DR needs into the three standards that they developed. This standards structure made documentation and training far easier than if each system had its own unique recovery procedures, RTOs, and RPOs.



Developing business-driven standards not only provides consistency that lowers TCO (total cost of operations), the organization also gets disaster recovery capabilities that actually meet business needs.

## *Maintaining DR Documentation*

The consummation of disaster recovery planning is the completed disaster recovery plan and recovery procedures. Those written documents are the culmination of a great deal of effort that has a single purpose — the survival of the organization in the face of a disaster.

In the following sections, I discuss many facets of DR documents, including

- ✓ How to manage documents
- ✓ How to update documents
- ✓ How to publish and distribute documents

Many people look at documentation as a necessary but altogether evil pastime. Although it may be mundane at times, it's the central fixture of disaster recovery planning. You have to get it right because the survival of your organization depends on it!



## *Managing DR documents*

Document management is a lifecycle proposition. Given the document-centric nature of disaster recovery planning, you need to keep those DR documents locked up safe and allow only authorized and qualified individuals to touch them. Seriously — treat high-value documents such as Business Impact Analyses (BIAs) and DR procedures as reverently as software source code.

### *Protecting DR documents*

Protect the official DR source documents so only authorized people can access them. Ideally, you should keep them in a *vault* — a database that's a part of a document management system. Authorized people must identify themselves by logging in before they can perform any operations on any DR documents.

### *Managing official DR documents*

You need to manage official DR documents, including Business Impact Analyses, DR procedures, and many more, through manual or automated means. The document management process should include these basic functions:

- ✓ **Check out:** When someone needs to make changes to a document, they first have to check out the document from the doc management system. After someone checks out a document, the doc management system optionally blocks others from checking out the same document until the person who first checked it out returns it. Whether you program the doc management system to block others from checking out the document is a policy decision that you make when you set up that system.
- ✓ **Review:** When a person makes changes to a document, he or she can circulate it for review by others in the organization. A full-featured doc management system may handle this review automatically, capturing comments and perhaps even proposing changes.
- ✓ **Check in:** After the document author receives and incorporates comments from others, he or she can finalize the document and check it back in to the system. When a person tries to check in a document, most doc management systems query that person for several pieces of information:
  - **Change reason:** A few words describing the change, such as ERP Upgrade or Migration to Hitachi SAN.
  - **Change description:** A longer description of the change — a couple of sentences.
  - **Author:** Name of the person who made the change, usually the person checking in the document.

## 258 Part III: Managing Recovery Plans

- **Version number:** Some document management systems create and increment version numbers automatically, others don't.
- **Approved by:** The name of the person or group who approved the changes.
- **Reviewed by:** The name of the person(s) who reviewed the document.

- ✓ **Update:** Sometimes tied to check in, an update causes a newly checked-in document to become the new official document. You can think of updating as a make current function that identifies a version of a document as the official version.
- ✓ **Version history:** A function that permits the user (not just anyone, but someone authorized to access the document management system) to view information about each prior version of a document.
- ✓ **Retrieve older version:** Doc management systems permit an authorized user to retrieve an older version of a document.

Doc management systems have many other functions associated with the management of documents under their control. The preceding list describes only the common functions that these systems use.



If your organization doesn't have a formal document management system, you can perform these steps manually by storing versions of documents on a file server and using spreadsheets or other means for tracking document activities such as check ins, check outs, and updates.

### ***Document content***

Any official documentation should have a consistent style and appearance, DR documentation included. Elements such as headers, footers, versions, and modification history are all vital to the integrity of DR documents. I discuss this topic fully in Chapter 9.

## ***Updating DR documents***

When you make the decision to update a DR document, you assign someone to actually perform this task.

Updating a DR procedure involves more than just editing the changes into the document. The document editor needs to perform some tasks, or read system or process documentation, to understand exactly how to change the content in the procedure. He or she might need to test the procedure on a test system to make sure the document describes the procedure accurately. He or she might need to include screen shots and other actions for clarity.

In terms of the actual document editing, the word processing program will need to be configured to show the changes made to the document. In Microsoft Word, this feature is called *Track Changes*; in FrameMaker, it's called *Track Edited Text*. This important feature permits reviewers (either other staff members or outsiders) to easily see precisely what changes have been made to a document. This is an example of a sentence that's been added. ~~This sentence has been removed.~~



Highlighting changes that are made to a document does have a disadvantage: Reviewers might focus too much on the changes and lose sight of the entire procedure. Document reviewers need to understand their responsibilities and know that they're checking not just for grammar, but for accuracy. And who knows — they might even be the ones who perform the procedure in an actual disaster!

When the document editor finishes making changes to the DR document, he or she can perform whatever check-in and updating tasks your organization uses.



After changes have been made to a DR procedure, you may need to test that procedure. Someone in the organization needs to track these updates and make decisions about when you need to test the recovery procedure if significant changes are made. A DR program doesn't run itself — it needs some management oversight so important activities don't fall through the cracks.

Set up a document review calendar that includes some sort of reminders for staff members to review documents in the DR library. Here's a suggested calendar for review:

- ✓ **Emergency contact lists — monthly:** Attrition and organization changes may happen frequently enough that you need to work hard to keep these lists fresh. Sometimes, people simply change their office, mobile, and home phone numbers, as well.
- ✓ **Recovery procedures — quarterly:** Little and big changes in applications and supporting environments may affect the accuracy of recovery documents.
- ✓ **Architecture documents — quarterly:** Document changes in application and infrastructure architecture so recovery personnel can become familiar with the architecture supporting each application's native environment.
- ✓ **Business Impact Analysis (BIA) — annually:** Changes in business priorities and market conditions may influence recovery objectives, such as your Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

## 260 Part III: Managing Recovery Plans

### *Publishing and distributing documents*

After you update DR documents, particularly recovery procedure documents, key personnel need to know about these changes.

For most ordinary documents, you simply update the document and make it available via your business's customary means (a file server or portal, for instance). But DR documents, especially procedures, aren't ordinary documents. You need to do more than simply publish them and let people download them at their leisure. The following sections explain.

#### ***Registered users***

Send all disaster recovery documents' updates to all registered users via e-mail or whatever means are right for your organization.

Disaster recovery procedure documents (as well as others that I mention in the following list) are so important that members of recovery teams need to have their own soft copies and maybe even hardcopies.

Someone needs to actively manage the list of recovery team members and others who need the newest versions of recovery procedures and other documents. Tracking users is tedious and mundane, but the survival of the organization may depend on it.

Here are the documents that you need to publish and send to registered users:

- ✓ **All recovery procedure documents:** 'Nuff said.
- ✓ **Updated architecture documents:** Descriptions and diagrams about how individual applications, networks, systems, and the entire environment is put together and how it works.
- ✓ **Emergency contact lists:** Essential for all recovery personnel, particularly in disasters in which communications are affected.
- ✓ **Communications procedures:** If the DR team has developed procedures for emergency communications, you need to keep this document fresh and in everyone's hands.
- ✓ **Wallet cards:** If you maintain wallet cards with essential contact info, you must send new versions with updated names and contact info to registered users whenever you update those cards.
- ✓ **Indexes to more documents:** The organization needs to maintain copies of documentation that hardware and software vendors produce so recovery teams can have easy access to product manufacturers' documentation, even during a disaster when communications may not be so good.

### *Recordkeeping*

Keep detailed records about all document updates, including the individual names of people who send hardcopies (or CD-ROM, or whatever form) to whom and when. These and other records that an organization's DR program produce are vital, and you must care for them well. Keeping accurate records helps to ensure that DR documents are well managed and distributed to all the right people. Ensure that these records are always up to date, accurate, and available to everyone who's authorized to access them by using good document management practices, as well as security and backups.

## *Training Response Teams*

You may have noticed that this section is short, and I have a good reason for it. But I'm not going to give the secret away just yet. You need to understand enough about DRP so you don't have to come running back to this book every time you need an answer (but I also don't want this book to gather dust on your shelf — that would be an equally tragic outcome).

Over in Chapter 10, I discuss testing DR plans. Done properly, performing those tests can take care of the training issue, all by itself.

### *Types of training*

Company staff have several levels of training available:

- ✓ **Paper testing:** Circulate recovery procedures to a fairly wide audience. Include all the personnel who are likely perform the actual recovery effort. By carefully reading and testing the recovery documents, they mentally step through the recovery procedures.
- ✓ **Walkthroughs:** You can use these group events to indoctrinate new staff members and refresh existing staff with disaster recovery procedures. New faces can introduce new knowledge and wisdom, which benefits all parties.
- ✓ **Parallel tests:** There's nothing like hands-on testing to keep recovery personnel familiar with recovery procedures. New staff members benefit from parallel testing by observing more experienced staffers in action.
- ✓ **Cutover tests:** A cutover test is a kind of controlled crisis — or, at least, a scheduled crisis in which the stakes are high. Personnel can benefit from the intensity of the experience.

## 262 Part III: Managing Recovery Plans

Practice makes perfect. If you carefully and properly choose the participants for each type of test, simply performing the test provides the participants with the necessary training.

### *Indoctrinating new trainees*

Train new employees in the organization, particularly those who are likely to be on recovery teams, as soon as possible. I suggest the following scheme for getting new staff members up to speed on recovery procedures:

- ✓ **Procedure review — week one:** Make one of the earliest assignments for new staff members a review of all DR recovery procedure documents.
- ✓ **Business Impact Analysis (BIA):** Have new staff members read through the BIA to help them see the big picture about the business's critical processes.
- ✓ **Walkthroughs:** Invite new staff members to walkthroughs, even if they're only observers. Observing a walkthrough exposes them to the thought behind the BIA and the recovery plans and procedures.
- ✓ **Simulations:** See what kind of management and leadership skills your new staff members may possess.
- ✓ **Parallel and cutover tests:** Involving new staff members in these tests spreads the experience around. You never know who'll be available to help out in an actual disaster, so the more people who have hands-on experience, the better.
- ✓ **Formal goals and milestones:** If you incorporate involvement in all levels of testing as part of employee goals and milestones, you give new employees additional incentive to get involved and up to speed. You also send a message that the organization is serious about disaster recovery planning.
- ✓ **Formal and informal training:** Introduce new employees to the culture of disaster recovery planning in the organization by setting up formal training classes and brown-bag lunch events.

The activities in the preceding list can help influence new employees early, and many organizations make preparation for disaster a top priority.

You probably don't need to develop an entire curriculum for training potential recovery personnel. Just include them in all of the review, revision, and testing activities that need to take place, and they can get their training through OJT (on-the-job training).