CHAPTER 9

Business Continuity and Disaster Recovery

This chapter presents the following:

- Project initiation steps
- Recovery and continuity planning requirements
- Business impact analysis
- Selecting, developing, and implementing disaster and continuity plans
- Backup and offsite facilities
- Types of drills and tests

We can’t prepare for every possibility, as recent events have proved. In 2005, Hurricane Katrina carried out extensive damage. Businesses were not merely affected—their buildings were destroyed and lives were lost. The catastrophic Indian Ocean tsunami that took place in December 2004 struck with complete surprise. The World Trade Center towers coming down after terrorists crashed planes into them affected many surrounding businesses, U.S. citizens, the government, and the world in a way that most people would have never imagined. Every year, thousands of businesses are affected by floods, fires, tornadoes, terrorist attacks, and vandalism in one area or another. The companies that survive these traumas are the ones that thought ahead, planned for the worst, estimated the possible damages that could occur, and put the necessary controls in place to protect themselves. This is a very small percentage of businesses today. Most businesses affected by these events have to close their doors forever. The companies that have survived these negative eventualities had a measured, approved set of advance arrangements and procedures.

An organization is dependent upon resources, personnel, and tasks that are performed on a daily basis in order to stay healthy, happy, and profitable. Most organizations have tangible resources, intellectual property, employees, computers, communication links, facilities, and facility services. If any one of these is damaged or inaccessible for one reason or another, the company can be crippled. If more than one is damaged, the company may be in a darker situation. The longer these items are unusable, the longer it will probably take for an organization to get back on its feet. Some companies are never able to recover after certain disasters. However, the companies that thought ahead, planned for the possible disasters, and did not put all of their eggs in one basket have had a better chance of resuming business and staying in the market.
Business Continuity and Disaster Recovery

What do we do if everything blows up? And how can we still make our widgets?

The goal of disaster recovery is to minimize the effects of a disaster and take the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner. This is different from continuity planning, which provides methods and procedures for dealing with longer-term outages and disasters. The goal of a disaster recovery plan is to handle the disaster and its ramifications right after the disaster hits; the disaster recovery plan is usually very information technology (IT) focused.

A disaster recovery plan is carried out when everything is still in emergency mode and everyone is scrambling to get all critical systems back online. A business continuity plan (BCP) takes a broader approach to the problem. It includes getting critical systems to another environment while repair of the original facilities is underway, getting the right people to the right places, and performing business in a different mode until regular conditions are back in place. It also involves dealing with customers, partners, and shareholders through different channels until everything returns to normal. So, disaster recovery deals with, “Oh my goodness, the sky is falling,” and continuity planning deals with, “Okay, the sky fell. Now, how do we stay in business until someone can put the sky back where it belongs?”

There is a continual theme throughout many of the chapters in this book: availability, integrity, and confidentiality. Because each chapter deals with a different topic, each looks at these three security characteristics in a slightly different way. In Chapter 4, for example, which discussed access control, availability meant that resources should be available to users and subjects in a controlled and secure manner. The access control method should protect the integrity and/or confidentiality of a resource. In fact, the access control method must take many steps to ensure the resource is kept confidential and that there is no possibility its contents can be altered while they are being accessed. In this chapter, we point out that integrity and confidentiality must not only be considered in everyday procedures, but in those procedures undertaken immediately after a disaster or disruption. For instance, it may not be appropriate to leave a server that holds confidential information in one building while everyone else moves to another building.

It is also important to note that a company may be much more vulnerable after a disaster hits, because the security services used to protect it may be unavailable or operating at a reduced capacity. Therefore, it is important that if the business has secret stuff, it stays secret and that the integrity of data and systems is ensured even when people and the company are in dire straits. Availability is one of the main themes behind business continuity planning in that it ensures that the resources required to keep the business going will continue to be available to the people and systems that rely upon them. This may mean backups need to be done religiously and that redundancy needs to be factored into the architecture of the systems, networks, and operations. If communication lines are disabled or if a service is rendered unusable for any significant period of time, there must be a quick and tested way of establishing alternate communications and services.
When looking at business continuity planning, some companies focus mainly on backing up data and providing redundant hardware. Although these items are extremely important, they are just small pieces of the company’s overall operations pie. Hardware and computers need people to configure and operate them, and data is usually not useful unless it is accessible by other systems and possibly outside entities. Thus, a larger picture of how the various processes within a business work together needs to be understood. Planning must include getting the right people to the right places, documenting the necessary configurations, establishing alternate communications channels (voice and data), providing power, and making sure all dependencies, including processes and applications, are properly understood and taken into account. For example, there may be no point in bringing a server back online if the DNS server is not working on the network.

It is also important to understand how automated tasks can be carried out manually, if necessary, and how business processes can be safely altered to keep the operation of the company going. This may be critical in ensuring the company survives the event with the least impact to its operations. Without this type of vision and planning, when a disaster hits, a company could have its backup data and redundant servers physically available at the alternate facility, but the people responsible for activating them may be standing around in a daze not knowing where to start or how to perform in such a different environment.

**Business Continuity Planning**

Preplanned procedures allow an organization to:

- Provide an immediate and appropriate response to emergency situations
- Protect lives and ensure safety
- Reduce business impact
- Resume critical business functions
- Work with outside vendors during recovery period
- Reduce confusion during a crisis
- Ensure survivability of the business
- Get “up and running” quickly after a disaster

Part of business decisions today should include the following:

- Letting business partners know your company is prepared
- Reassuring shareholders and boards of trustees about your company’s readiness
- Making sure a BCP is in place if industry regulations require it


**Business Continuity Steps**

Although no specific scientific equation must be followed to create continuity plans, certain best practices have proven themselves over time. The National Institute of Standards and Technology (NIST) organization is responsible for developing these best practices and documenting them so they are easily available to all. NIST outlines the following steps in its Special Publication 800-34, *Continuity Planning Guide for Information Technology Systems* (http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf):

1. *Develop the continuity planning policy statement*. Write a policy that provides the guidance necessary to develop a BCP and that assigns authority to the necessary roles to carry out these tasks.

2. *Conduct the business impact analysis (BIA)*. Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities, threats, and calculate risks.

3. *Identify preventive controls*. Once threats are recognized, identify and implement controls and countermeasures to reduce the organization’s risk level in an economical manner.

4. *Develop recovery strategies*. Formulate methods to ensure systems and critical functions can be brought online quickly.

5. *Develop the contingency plan*. Write procedures and guidelines for how the organization can still stay functional in a crippled state.

6. *Test the plan and conduct training and exercises*. Test the plan to identify deficiencies in the BCP and conduct training to properly prepare individuals on their expected tasks.

7. *Maintain the plan*. Put in place steps to ensure the BCP is a living document that is updated regularly.

Different companies and guidelines include the previous information, but may have different names for the steps. (ISC)² has the following steps with the same information:

1. Project initiation
2. BIA
3. Recovery strategy
4. Plan design and development
5. Implementation
6. Testing
7. Continual maintenance
The necessary steps required to roll out a business continuity planning process are illustrated in Figure 9-1.

Although the NIST 800-34 document deals specifically with IT contingency plans, these steps are the same when creating enterprise-wide BCPs. This chapter steps you through these different phases and what you should do to build an effective and useful BCP.

References

- iNFSYSSEC Business Continuity and Disaster Recovery Planning resources page  www.infosyssec.net/infosyssec/buscon1.htm
Making BCP Part of the Security Policy and Program

Why do we need to combine business continuity and security plans anyway?
Response: They both protect the business, unenlightened one.

As explained in Chapter 3, every company should have security policies, procedures, standards, and guidelines. Having these in place is part of a well-managed environment, and brings forth operational and cost-savings benefits. Together, they provide the framework of a security program for an organization. As such, the program needs to be a living entity. As a company goes through changes, so should the program, thereby ensuring it stays current, usable, and effective.

Business continuity should be a part of the security program and business decisions, as opposed to being an entity that stands off in a corner by itself. When properly integrated with change management processes, it stands a much better chance of being continually updated and improved upon. Business continuity is a foundational piece of an effective security program and is critical to ensuring relevance in time of need.

A very important question to ask when first developing a BCP is why it is being developed. This may seem silly and the answer may at first appear obvious, but that is not always the case. One would think that the reason to have these plans is to deal with an
unexpected disaster and to get people back to their tasks as quickly and as safely as possible, but the full story is often a bit different. Why are most companies in business? To make money and be profitable. If these are usually the main goals of businesses, then any BCP needs to be developed to help achieve and, more importantly, maintain these goals. The main reason to develop these plans in the first place is to reduce the risk of financial loss by improving the company’s ability to recover and restore operations. This encompasses the goals of mitigating the effects of the disaster.

Not all organizations are businesses that exist to make profits. Government agencies, military units, nonprofit organizations, and the like exist to provide some type of protection or service to a nation or society. While a company must create its BCP to ensure that revenue continues to come in so it can stay in business, other types of organizations must create their BCPs to make sure they can still carry out their critical tasks. Although the focus and business drivers of the organizations and companies may differ, their BCPs often will have similar constructs—which is to get their critical processes up and running.

Protecting what is most important to a company is rather difficult if what is most important is not first identified. Senior management is usually involved with this step because it has a point of view that extends beyond each functional manager’s focus area of responsibility. The company’s business plan usually defines the company’s critical mission and business function. The functions must have priorities set upon them to indicate which is most crucial to a company’s survival.

For many companies, financial operations are most critical. As an example, an automotive company would be impacted far more seriously if its credit and loan services were unavailable for a day than if, say, an assembly line went down for a day, since credit and loan services are where it generates the biggest revenues. For other organizations, customer service might be the most critical area. For example, if a company makes heart pacemakers and its physician services department is unavailable at a time when an operating room surgeon needs to contact it because of a complication, the results could be disastrous for the patient. The surgeon and the company would likely be sued and the company would likely never be able to sell another pacemaker to that surgeon, her colleagues, or perhaps even the patient’s HMO ever again. It would be very difficult to rebuild a reputation and sales after something like that happened.

Advanced planning for emergencies covers issues that were thought of and foreseen. Many other problems may arise that are not covered in the plan; thus, flexibility in the plan is crucial. The plan is a systematic way of providing a checklist of actions that should take place right after a disaster. These actions have been thought through to help the people involved be more efficient and effective in dealing with traumatic situations.

The most critical part of establishing and maintaining a current continuity plan is management support. Management must be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support. The business case may include current vulnerabilities, regulatory and legal obligations, the current status of recovery plans, and recommendations. Management is mostly concerned with cost/benefit issues, so preliminary numbers need to be gathered and potential losses estimated. The decision of how a company should recover is purely a business decision and should always be treated as such.
**Project Initiation**

Before everyone runs off in 2000 different directions at one time, let’s understand what needs to be done in the project initiation phase. This is the phase in which the company really needs to figure out what it is doing and why. So, after someone gets the donuts and coffee, let’s get down to business.

Once management’s support is solidified, a *business continuity coordinator* must be identified. This will be the leader for the BCP team and will oversee the development, implementation, and testing of the continuity and disaster recovery plans. It is best if this person has good social skills, is somewhat of a politician, and has a cape, because he will need to coordinate a lot of different departments and busy individuals who have their own agendas. This person needs to have direct access to management and have the credibility and authority to carry out leadership tasks.

A leader needs a team, so a BCP committee needs to be put together. Management and the coordinator should work together to appoint specific, qualified people to be on this committee. The team must be comprised of people who are familiar with the different departments within the company, because each department is unique in its functionality and has distinctive risks and threats. The best plan is when all issues and threats are brought to the table and discussed. This cannot be done effectively with a few people who are familiar with only a couple of departments. Representatives from each department must be involved with not only the planning stages but also the testing and implementation stages.

The committee should be made up of representatives from *at least* the following departments:

- Business units
- Senior management
- IT department
- Security department
- Communications department
- Legal department

If the BCP coordinator is a good management leader, she will understand that it is best to make these team members feel a sense of ownership pertaining to their tasks and roles. The people who develop the BCP should also be the ones who execute it. If you knew that in a time of crisis you would be expected to carry out some critical tasks, you might pay more attention during the planning and testing phases.

The team must then work with the management staff to develop the ultimate goals of the plan, identify the critical parts of the business that must be dealt with first during a disaster, and ascertain the priorities of departments and tasks. Management needs to help direct the team on the scope of the project and the specific objectives. At first glance, it might seem as though the scope and objectives are quite clear—protect the company. But it is not that simple. Is the team supposed to develop a BCP for just one facility or for more than one facility? Is the plan supposed to cover just large potential threats (hurricanes, tornadoes, floods) or deal with smaller issues as well (loss of a communications line, power failure, Internet connection failure)? Should the plan address possible terror-
ist attacks and bomb threats? What is the threat profile of the company? If the scope of the project is not properly defined, how do you know when you are done?

**NOTE** Most companies outline the scope of their BCP to encompass only the larger threats. The smaller threats are then covered by independent departmental contingency plans.

At this phase, the team works with management to develop the *continuity planning policy statement*. This statement lays out the scope of the BCP project, the team member roles, and the goals of the project. Basically, it is a document that outlines what needs to be accomplished after the team communicates with management and comes to agreement on the terms of the project. The document should be returned to management to make sure there are no assumptions or omissions and that everyone is in agreement.

The BCP coordinator would then need to implement some good old-fashioned project management skills; see Table 9-1. A project plan should be developed that has the following components:

- Objective-to-task mapping
- Resource-to-task mapping
- Milestones
- Budget estimates
- Success factors
- Deadlines

Once the project plan is completed, it should be presented to management for written approval before any further steps are taken. It is important there are no assumptions in the plan and that the coordinator obtains permission to use the necessary resources to move forward.

<table>
<thead>
<tr>
<th>BCP Activity</th>
<th>Start Date</th>
<th>Required Completion Date</th>
<th>Completed? Initials/Date</th>
<th>Approved? Initials/Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiating the project</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuity policy statement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business impact analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify preventive controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery strategies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop BCP and DRP documents</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 9-1** Steps to Be Documented and Approved
Business Continuity Planning Requirements

A major requirement for anything that has such far-reaching ramifications as business continuity planning is management support. It is critical that management understands what the real threats are to the company, the consequences of those threats, and the potential loss values for each threat. Without this understanding, management may only give lip service to continuity planning, and in some cases that is worse than not having any plans at all because of the false sense of security it creates. Without management support, the necessary resources, funds, and time will not be devoted, which could result in bad plans that, again, may instill a false sense of security. Failure of these plans usually means a failure in management understanding, vision, and due-care responsibilities.

Executives may be held responsible and liable under various laws and regulations. They could be sued by stockholders and customers if they do not practice due diligence and due care and fulfill all of their responsibilities when it comes to disaster recovery and business continuity items. Organizations that work within specific industries have strict regulatory rules and laws that they must abide by, and these should be researched and integrated into the plan from the beginning. For example, banking and investment organizations must ensure that even if a disaster occurs, their customers’ confidential information will not be disclosed to unauthorized individuals or be altered or vulnerable in any way. Disaster recovery, continuity development, and planning work best in a top-down approach, not a bottom-up approach. This means that management, not the staff, should be driving the project.

Many companies are running so fast to try to keep up with a dynamic and changing business world that they may not see the immediate benefit of spending time and resources on disaster recovery issues. Those individuals who do see the value in these efforts may have a hard time convincing top management if management does not see a potential profit margin or increase in market share as a result. But if a disaster does hit and they did put in the effort to properly prepare, the result can literally be priceless. Today’s business world requires two important characteristics: the drive to produce a great product or service and get it to the market, and the insight and wisdom to know that unexpected trouble can easily find its way to one’s doorstep.

It is important that management set the overall goals of continuity planning, and it should help set the priorities of what should be dealt with first. Once management sets the goals, policies, and priorities, other staff members who are responsible for these plans can fill in the rest. However, management’s support does not stop there. It needs to make sure the plans and procedures developed are actually implemented. Management must make sure the plans stay updated and represent the real priorities—not simply those perceived—of a company, which change over time.

Business Impact Analysis

How bad is it going to hurt and how long can we deal with this level of pain?

Business continuity planning deals with uncertainty and chance. What is important to note here is that even though you cannot predict whether or when a disaster will happen, that doesn’t mean you can’t plan for it. Just because we are not planning for an earthquake to hit us tomorrow morning at 10 A.M. doesn’t mean we can’t plan the activities required to successfully survive when an earthquake (or a similar disaster) does hit.
The point of making these plans is to try to think of all the possible disasters that could take place, estimate the potential damage and loss, categorize and prioritize the potential disasters, and develop viable alternatives in case those events do actually happen.

A business impact analysis (BIA) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function’s criticality level. But how do we determine a classification scheme based on criticality levels? The BCP committee must identify the threats to the company and map them to the following characteristics:

- Maximum tolerable downtime
- Operational disruption and productivity
- Financial considerations
- Regulatory responsibilities
- Reputation

The committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know, which are department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks get accomplished within the organization, whether it’s a process, transaction, or service, along with any relevant dependencies. Process flow diagrams should be built, which will be used throughout the BIA and plan development stages.

Upon completion of the data collection phase, the BCP committee needs to conduct an analysis to establish which processes, devices, or operational activities are critical. If a system stands on its own, doesn’t affect other systems, and is of low criticality, then it can be classified as a tier two or three recovery step. This means these resources will not be dealt with during the recovery stages until the most critical (tier one) resources are up and running. This analysis can be completed using standard risk assessment and analysis methodologies. (For a full examination of risk analysis, refer to Chapter 3.)

Threats can be manmade, natural, or technical. A manmade threat may be an arsonist, a terrorist, or a simple mistake that can have serious outcomes. Natural threats may be tornadoes, floods, hurricanes, or earthquakes. Technical threats may be data corruption, loss of power, device failure, or loss of a data communications line. It is important to identify all possible threats and estimate the probability of them happening. Some issues may not immediately come to mind when developing these plans, such as an employee strike, vandals, disgruntled employees, or hackers, but they do need to be identified. These issues are often best addressed in a group with scenario-based exercises. This ensures that if a threat becomes reality, the plan includes the ramifications on all business tasks, departments, and critical operations. The more issues that are thought of and planned for, the better prepared a company will be if and when these events take place.
The committee needs to step through scenarios that could produce the following results:

- Equipment malfunction or unavailable equipment
- Unavailable utilities (HVAC, power, communications lines)
- Facility becomes unavailable
- Critical personnel become unavailable
- Vendor and service providers become unavailable
- Software and/or data corruption

The next step in the risk analysis is to assign a value to the assets that could be affected by each threat. This helps establish economic feasibility of the overall plan. As discussed in Chapter 3, assigning values to assets is not as straightforward as it seems. The value of an asset is not just the amount of money paid for it. The asset’s role to the company has to be considered, along with the labor hours that went into creating it if it is a piece of software. The value amount could also encompass the liability issues that surround the asset if it were damaged or insecure in any manner. (Review Chapter 3 for an in-depth description and criteria for calculating asset value.)
Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. The goal is to see exactly how a business will be affected by different threats. The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the company to ensure that the findings are appropriate and describe the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts.

Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

- Loss in reputation and public confidence
- Loss of competitive advantages
- Increase in operational expenses
- Violations of contract agreements
- Violations of legal and regulatory requirements
- Delayed income costs
- Loss in revenue
- Loss in productivity

These costs can be direct or indirect and must be properly accounted for.

So if the BCP team is looking at the threat of a terrorist bombing, it is important to identify which business function most likely would be targeted, how all business functions could be affected, and how each bulleted item in the loss criteria would be directly or indirectly involved. The timeliness of the recovery can be critical for business processes and the company’s survival. For example, it may be acceptable to have the customer support functionality out of commission for two days, whereas five days may leave the company in financial ruin.

After identifying the critical functions, it is necessary to find out exactly what is required for these individual business processes to take place. The resources that are required for the identified business processes are not necessarily just computer systems, but may include personnel, procedures, tasks, supplies, and vendor support. It must be understood that if one or more of these support mechanisms is not available, the critical function may be doomed. The team must determine what type of effect unavailable resources and systems will have on these critical functions.

The BIA identifies which of the company’s critical systems are needed for survival and estimates the outage time that can be tolerated by the company as a result of various unfortunate events. The outage time that can be endured by a company is referred to as the maximum tolerable downtime (MTD).
The following are some MTD estimates that may be used within an organization:

- **Nonessential** 30 days
- **Normal** Seven days
- **Important** 72 hours
- **Urgent** 24 hours
- **Critical** Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the company can survive without it. These estimates will help the company determine what backup solutions are necessary to ensure the availability of these resources. For example, if being without a T1 communication line for three hours would cost the company $130,000, the T1 line would be considered critical and thus the company should put in a backup T1 line from a different carrier. If a server going down and being unavailable for ten days will only cost the company $250 in revenue, this would fall into the normal category and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor service level agreement (SLA), which, for example, may promise to have it back online in eight days.

The BCP team must try to think of all possible events that might occur that could turn out to be detrimental to a company. The BCP team also must understand it cannot possibly contemplate all events, and thus protection may not be available for every scenario introduced. Being properly prepared specifically for a flood, earthquake, terrorist attack, or lightning strike is not as important as being properly prepared to respond to *anything* that damages or disrupts critical business functions.

All of the previously mentioned disasters could cause these results, but so could a meteor strike, a tornado, or a wing falling off of a plane passing overhead. So the moral to the story is to be prepared for the loss of any or all business resources, instead of focusing on the events that could cause the loss.

**NOTE** A BIA is performed at the beginning of business continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the company’s critical systems needed for survival and estimates the outage time that can be tolerated by the company as a result of a disaster or disruption.
Interdependencies

Operations depend on manufacturing, manufacturing depends on R&D, payroll depends on accounting, and they all depend on IT.

Response: Hold on. I need to write this down.

It is important to look at a company as a complex animal instead of a static two-dimensional entity. It comprises many types of equipment, people, tasks, departments,
communications mechanisms, and interfaces to the outer world. The biggest challenge of true continuity planning is understanding all of these intricacies and their interrelationships. A team may develop plans to back up and restore data, implement redundant data processing equipment, educate employees on how to carry out automated tasks manually, and obtain redundant power supplies. But if all of these components don’t know how to work together in a different environment to get the products out the door, it might all be a waste of time.

The following interrelation and interdependency tasks should be carried out by the BCP team and addressed in the resulting plan:

- Define essential business functions and supporting departments.
- Identify interdependencies between these functions and departments.
- Discover all possible disruptions that could affect the mechanisms necessary to allow these departments to function together.
- Identify and document potential threats that could disrupt interdepartmental communication.
- Gather quantitative and qualitative information pertaining to those threats.
- Provide alternative methods of restoring functionality and communication.
- Provide a brief statement of rationale for each threat and corresponding information.

The main goal of business continuity is to resume business as quickly as possible, spending the least amount of money. The overall business interruption and resumption plan should cover all organizational elements, identify critical services and functions, provide alternatives for emergency operations, and integrate each departmental plan. This can be accomplished by in-house appointed employees, outside consultants, or a combination of both. A combination can bring many benefits to the company, because the consultants are experts in this field and know the necessary steps, questions to ask, and issues to look for, and offer general reasonable advice, whereas in-house employees know their company intimately and have a full understanding of how certain threats can affect operations. It is good to cover all the necessary ground, and many times a combination of consultants and employees provides just the right recipe.

### Enterprise-wide

The agreed-upon scope of the BCP will indicate if one or more facilities will be included in the plan. Most BCPs are developed to cover the enterprise as a whole, instead of dealing with only portions of the organization. In larger organizations, it can be helpful for each department to have its own specific contingency plan that will address its specific needs during recovery. These individual plans need to be compatible with the enterprise-wide BCP.
Up until now, we have established management’s responsibilities as the following:

- Committing fully to the BCP
- Setting policy and goals
- Making available the necessary funds and resources
- Taking responsibility for the outcome of the development of the BCP
- Appointing a team for the process

The BCP team’s responsibilities are as follows:

- Identifying regulatory and legal requirements that must be met
- Identifying all possible vulnerabilities and threats
- Estimating the possibilities of these threats and the loss potential
- Performing a BIA
- Outlining which departments, systems, and processes must be up and running before any others
- Developing procedures and steps in resuming business after a disaster

Several software tools are available for developing a BCP that simplify the process. Automation of these procedures can quicken the pace of the project and allow easier gathering of the massive amount of information. Many of the necessary items are provided in the boilerplate templates.

This information, along with other data explained in previous sections, should be presented to senior management. Management usually wants information stated in monetary, quantitative terms, not in subjective, qualitative terms. It is one thing to know that if a tornado were to hit, the result would be really bad, but it is another to know that if a tornado were to hit and affect 65 percent of the facility, the company could be at risk of losing computing capabilities for up to 72 hours, power supply for up to 24 hours, and a full stop of operations for 76 hours, which would equate to a loss of $125,000 each day. Management has a much harder time dealing with really bad than with real numbers.

It is important to realize that up until now, the BCP team has not actually developed any of its BCP. It has been collecting data, carrying out analysis on this data, and presenting it to management. Management must review these findings and give the “okay” for the team to move forward and actually develop the plan. In our scenario, we will assume that management has given the thumbs up and the team will now move into the next stages.

References

- Business Continuity Institute (BCI) www.thebci.org
- DRI International (DRII) www.drii.org
Preventive Measures

Let’s just wait and see if a disaster hits.
Response: How about we be more proactive?

During the BIA, the BCP team identified the maximum tolerable downtime for the critical resources. This was done to understand the business impact that would be caused if the assets were unavailable for one reason or another. It only makes sense that the team would try to reduce this impact and mitigate these risks by implementing preventive measures. Not implementing preventive measures would be analogous to going to a doctor, being told to stop eating 300 candy bars a day, increase physical activities, and start taking blood pressure medicine, and then choosing not to follow any of these preventive measures. Why go to the doctor in the first place? The same concept holds true with companies. If a team has been developed to identify risks and has come up with solutions, but the company does not implement at least some of these solutions, why put this team together in the first place?

So, instead of just waiting for a disaster to hit to see how the company holds up, countermeasures should be integrated to better fortify the company from the impacts that were recognized. Appropriate and cost-effective preventive methods and proactive measures are more preferable than reactionary methods. Which types of preventive mechanisms should be put in place depends upon the results of the BIA, but they may include some of the following components:

- Fortification of the facility in its construction materials
- Redundant servers and communications links
- Power lines coming in through different transformers
- Redundant vendor support
- Purchasing of insurance
- Purchasing of UPS and generators
- Data backup technologies
- Media protection safeguards
- Increased inventory of critical equipment
- Fire detection and suppression systems

NOTE  Many of these controls are discussed in this chapter, but others are covered in Chapter 6 and Chapter 12.

Recovery Strategies

Up to this point, the BCP team has carried out the project initiation phase. In this phase, the team obtained management support, the necessary resources, laid out the scope of the project, and identified the BCP team. It also completed the BIA phase. This
means that the committee carried out a risk assessment and analysis, which resulted in a report of the real risk level the company faces.

The BCP committee already had to figure out how the organization works as a whole in its BIA phase. It drilled down into the organization and identified the critical functions that absolutely have to be up and running for the company to continue operating. It identified the resources these functions require and calculated MTD values for the individual resources and the functions themselves. So it may seem as though the BIA phase is already completed. But when the BCP committee carried out these tasks, it was in the “risk assessment” phase of the BCP process. Its goals were to figure out how bad the company could be hurt in different disaster scenarios.

In the recovery strategy stage, the team approaches this information from a different perspective. It now has to figure out what the company needs to do to actually recover the items it has identified as being so important to the organization overall. The BIA provides the blueprint for the recovery strategies for all the components, because the business processes are totally dependent upon these other recovery strategies to take place properly.

At this point, the findings from the BIA have been reported to management and management has allocated the necessary resources to move into the next phases. The BCP committee now must discover the most cost-effective recovery mechanisms that need to be implemented to address the threats identified in the BIA stage. Remember that in the BIA phase, the team calculated the potential losses for each identified threat. (If the facility was unavailable, it would cost the organization $200,000 a day; if the Internet connection went down, it would cost the company $12,000 per hour, and so on.) The team will use these values in its cost-benefit analysis when reviewing and choosing the necessary recovery solutions that need to be put into place to mitigate the organization’s risk level.

So what does the BCP team need to accomplish in the recovery strategy stage? The team needs to actually define the recovery strategies, which are a set of predefined activities that will be implemented and carried out in response to a disaster. Sounds simple enough, but in reality this phase requires just as much work as the BIA phase.

What Is the Difference Between Preventive Measures and Recovery Strategies?

Preventive mechanisms are put into place to try to reduce the possibility of the company experiencing a disaster and, if a disaster does hit, to lessen the amount of damage that will take place. Although the company cannot stop a tornado from coming, it could choose to move its facility from tornado valley in Kansas. The company cannot stop a car from plowing into and taking out a transformer, but it can have a separate feed from a different transformer in case this happens.

Recovery strategies are processes on how to rescue the company after a disaster takes place. These processes will integrate mechanisms such as establishing alternate sites for facilities, implementing emergency response procedures, and possibly activating the preventive mechanisms that have already been implemented.
In the BIA, the team has calculated the necessary recovery times that must be met for the different critical business functions and the resources those functions rely upon. For example, let's say the team has figured out it would cost the company $200,000 per day in lost revenue if its facility were destroyed and unusable. Now the team knows that the company has to be up and running within five to six hours or the company could be financially crippled. This would mean that the company needs to obtain a hot site or redundant facility that would allow it to be up and running in this amount of time.

The team has figured out these types of timelines for the individual business functions, operations, and resources. Now it has to identify the recovery mechanisms and strategies that must be implemented to make sure everything is up and running within the timelines it has calculated. The team needs to break down these recovery strategies into the following sections:

- Business process recovery
- Facility recovery
- Supply and technology recovery
- User environment recovery
- Data recovery

**Business Process Recovery**

A business process is a set of interrelated steps linked through specific decision activities to accomplish a specific task. Business processes have starting and ending points and are repeatable. The processes should encapsulate the knowledge of services, resources, and operations provided by a company. For example, when a customer requests to buy a car via an organization’s e-commerce site, a set of steps must be followed, such as these:

1. Validate that the car is available.
2. Validate where the car is located and how long it would take to ship it to the destination.
3. Provide the customer with the price and delivery date.
4. Accept the customer’s credit card information.
5. Validate and process the credit card order.
6. Send a receipt and tracking number to the customer.
7. Send the order to the car inventory location.
8. Restock inventory.
9. Send the order to accounting.

The BCP team needs to understand these different steps of the company’s most critical steps. The data are usually presented as a workflow document that contains the roles and resources needed for each process. The BCP team must understand the following about critical business processes:
Chapter 9: Business Continuity and Disaster Recovery

- Required roles
- Required resources
- Input and output mechanisms
- Workflow steps
- Required time for completion
- Interfaces with other processes

This will allow the team to identify threats and the controls to ensure the least amount of impact pertaining to process interruption.

Facility Recovery

*That mean storm hurt our office. Let’s go find another building to work in.*

Disruptions are of three main types: nondisasters, disasters, and catastrophes. A *nondisaster* is a disruption in service due to a device malfunction or failure. The solution could include hardware, software, or file restoration. A *disaster* is an event that causes the entire facility to be unusable for a day or longer. This usually requires the use of an alternate processing facility and restoration of software and data from offsite copies. The alternate site must be available to the company until its main facility is repaired and usable. A *catastrophe* is a major disruption that destroys the facility altogether. This requires both a short-term solution, which would be an offsite facility, and a long-term solution, which may require rebuilding the original facility.

Disasters and catastrophes are rare compared to nondisasters, thank goodness. Nondisasters can usually be taken care of by replacing a device or restoring files from onsite backups. The BCP team needs to think through onsite backup requirements and make well-informed decisions. The team must identify the critical equipment and estimate the mean time between failures (MTBF) and the mean time to repair (MTTR) to provide the necessary statistics of when a device may be meeting its maker and a new device may be required.

**NOTE**  
MTBF is the estimated lifetime of a piece of equipment and is calculated by the vendor of the equipment or a third party. The reason for using this value is to know approximately when a particular device will need to be replaced. MTTR is an estimate of how long it will take to fix a piece of equipment and get it back into production. These concepts are further explained in Chapter 12.

For larger disasters that affect the primary facility, an offsite backup facility must be accessible. Generally, contracts are established with third-party vendors to provide such services. The client pays a monthly fee to retain the right to use the facility in a time of need and then incurs a large activation fee when the facility actually has to be used. In addition, there would be a daily or hourly fee imposed for the duration of the stay. This is why subscription services for backup facilities should be considered a short-term solution, not a long-term solution.
It is important to note that most recovery site contracts do not promise to house the company in need at a specific location, but rather promise to provide what has been contracted for somewhere within the company’s locale. On, and subsequent to, September 11, 2001, many organizations with Manhattan offices were surprised when they were redirected by their backup site vendor, not to sites located in New Jersey (which were already full), but rather to sites located in Boston, Chicago, or Atlanta. This adds yet another level of complexity to the recovery process, specifically the logistics of transporting people and equipment to locations originally unplanned for.

Companies can choose from three main types of leased or rented offsite facilities:

- **Hot site**  A facility that is leased or rented and is fully configured and ready to operate within a few hours. The only missing resources from a hot site are usually the data, which will be retrieved from a backup site, and the people who will be processing the data. The equipment and system software must absolutely be compatible with the data being restored from the main site and must not cause any negative interoperability issues. These sites are a good choice for a company that needs to ensure a site will be available for it as soon as possible.

  Most hot-site facilities support annual tests that can be done by the company to ensure the site is functioning in the necessary state. This is the most expensive of the three types of offsite facilities and can have problems if a company requires proprietary or unusual hardware or software.

  **NOTE**  The vendor of a hot site will provide the most commonly used hardware and software products to attract the largest customer base. This will most likely not include one specific customer’s proprietary or unusual hardware or software products.

- **Warm site**  A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. In other words, a warm site is usually a hot site without the expensive equipment. Staging a facility with duplicate hardware and computers configured for immediate operation is extremely expensive, so a warm site provides an alternate facility with some peripheral devices. This is the most widely used model. It is less expensive than a hot site and can be up and running within a reasonably acceptable time period. It may be a better choice for companies that depend upon proprietary and unusual hardware and software, because they will bring their own hardware and software with them to the site after the disaster hits. The odds of finding a remote site vendor that would have a Cray supercomputer readily available in a time of need are pretty slim. The drawback, however, is that the annual testing available with hot-site contracts is not usually available with warm-site contracts and thus a company cannot be certain that it will in fact be able to return to an operating state within hours.

- **Cold site**  A leased or rented facility that supplies the basic environment, electrical wiring, air conditioning, plumbing, and flooring, but none of the equipment or additional services. It may take weeks to get the site activated and ready for work. The cold site could have equipment racks and dark fiber
(fiber that does not have the circuit engaged) and maybe even desks, but would require the receipt of equipment from the client, since it does not provide any. The cold site is the least expensive option but takes the most time and effort to actually get up and functioning right after a disaster. Cold sites are often used as backups for call centers, manufacturing plants, and other services that either can be moved lock, stock, and barrel in one shot or would require extensive retooling and building.

**NOTE** It is important to understand that the different site types listed here are provided by service bureaus, meaning a company pays a monthly subscription fee to another company for this space and service. A hot site is a subscription service. A redundant site is a site owned and maintained by the company, meaning the company does not pay anyone else for the site. A redundant site might be “hot” in nature, meaning it is ready for production quickly, but the CISSP exam differentiates between a hot site (subscription service) and a redundant site (owned by the company).

Most companies use warm sites, which have some devices such as disk drives, tape drives, and controllers, but very little else. These companies usually cannot afford a hot site, and the extra downtime would not be considered detrimental. A warm site can provide a longer-term solution than a hot site. Companies that decide to go with a cold site must be able to be out of operation for a week or two. The cold site usually includes power, raised flooring, climate control, and wiring.

The following provides a quick overview of the differences between offsite facilities:

**Hot Site Advantages**
- Ready within hours for operation
- Highly available
- Usually used for short-term solutions, but available for longer stays
- Annual testing available

**Hot Site Disadvantages**
- Very expensive
- Limited on hardware and software choices

**Warm and Cold Site Advantages**
- Less expensive
- Available for longer timeframes because of the reduced costs
- Practical for proprietary hardware or software use

**Warm and Cold Site Disadvantages**
- Not immediately available
- Operational testing not usually available
- Resources for operations not immediately available
Tertiary Sites
During the BIA phase, the team may recognize the danger of the primary backup facility not being available when needed, which could require a tertiary site. This is a secondary backup site, just in case the primary backup site is unavailable. The secondary backup site is sometimes referred to as a “backup to the backup.” This is basically plan B if plan A does not work out.

Backup tapes or other media should be tested periodically on the equipment kept at the hot site to make sure the media is readable by those systems. If a warm site is used, the tapes should be brought to the original site and tested on those systems. The reason for the difference is that when a company uses a hot site, it depends on the sys-
Offsite Location

When choosing a backup facility, it should be far enough away from the original site so one disaster does not take out both locations. In other words, it is not logical to have the backup site only a few miles away if the company is concerned about tornado damage, because the backup site could also be affected or destroyed. There is a rule of thumb that suggests that alternate facilities should be at a bare minimum at least five miles away from the primary site, while 15 miles is recommended for most low-to-medium critical environments, and 50–200 miles is recommended for critical operations to give maximum protection in cases of regional disasters.

Reciprocal Agreements

*If my facility is destroyed, can I come over to yours?*
*Response: Only if you bring hot cocoa and popcorn.*

Another approach to alternate offsite facilities is to establish a reciprocal agreement, also referred to as mutual aid, with another company. This means that company A agrees to allow company B to use its facilities if company B is hit by a disaster, and vice versa. This is a cheaper way to go than the other offsite choices, but it is not always the best choice. Most environments are maxed out pertaining to the use of facility space, resources, and computing capability. To allow another company to come in and work out of the same shop could prove to be detrimental to both companies. The stress of two companies working in the same environment could cause tremendous levels of tension. If it did work out, it would only provide a short-term solution. Configuration management could be a nightmare, and the mixing of operations could introduce many security issues.

If you allow another company to move into your facility and work from there, you may have a solid feeling about your friend, the CEO, but what about all of her employees whom you do not know? Now you have a new subset of people who may need to have privileged and direct access to your resources in the shared environment. This other company could be your competitor in the business world, so many of the employees may see you and your company more as a threat than one that is offering a helping hand in need. Close attention needs to be paid when assigning these other people access rights and permissions to your critical assets and resources, if they need access at all.

Reciprocal agreements have been known to work well in specific businesses, such as newspaper printing. These businesses require very specific technology and equipment that will not be available through any subscription service. These agreements follow a “you scratch my back and I’ll scratch yours” mentality. For most other organizations, they are generally, at best, a secondary option for disaster protection. The other issue to consider is that these agreements are not enforceable. This means that although company A said company B could use its facility when needed, when the need arises, company A legally does not have to fulfill this promise. However, there are still many companies who do opt for this solution either because of the appeal of low cost or, as noted earlier, because it may be the only viable solution in some cases.
Important issues need to be addressed before a disaster hits if a company decides to participate in a reciprocal agreement with another company:

- How long will the facility be available to the company in need?
- How much assistance will the staff supply in integrating the two environments and ongoing support?
- How quickly can the company in need move into the facility?
- What are the issues pertaining to interoperability?
- How many of the resources will be available to the company in need?
- How will differences and conflicts be addressed?
- How does change control and configuration management take place?
- How often can drills and testing take place?
- How can critical assets of both companies be properly protected?

**Redundant Sites**

*It’s mine and mine alone.*

*Response: Okay, keep it then.*

Some companies choose to have redundant sites, meaning one site is equipped and configured exactly like the primary site, which serves as a redundant environment. These sites are owned by the company and are mirrors of the original production environment. This is one of the most expensive backup facility options, because a full environment must be maintained even though it usually is not used for regular production activities until after a disaster takes place that triggers the relocation of services to the redundant site. But expensive is relative here. If the company would lose a million dollars if it were out of business for just a few hours, the loss potential would override the cost of this option. Many organizations are subjected to regulations that dictate they must have redundant sites in place, so expense is not an issue in these situations.

Another type of facility-backup option is a rolling hot site, or mobile hot site, where the back of a large truck or a trailer is turned into a data processing or working area. The trailer has all of the necessary power, telecommunications, and systems to allow for processing to take place right away. The trailer can be brought to the company’s parking lot or another location. Another, similar solution is a prefabricated building that can be easily and quickly put together. Military organizations and large insurance companies typically have rolling hot sites or trucks preloaded with equipment because they often need the flexibility to quickly relocate some or all of their processing facilities to different locations around the world depending on where the need arises.

Another option for organizations is to have multiple processing centers. An organization may have ten different facilities throughout the world, which may include products and technologies that would move all data processing from one facility to another in a matter of seconds when an interruption is detected. This technology can be implemented within the organization or from one facility to a third-party facility. Certain service bureaus provide this type of functionality to their customers. So if a company’s data processing is interrupted, all or some of the processing can be moved to the service bureau’s servers.
It is best if a company is aware of all available options for hardware and facility backups, to ensure it makes the best decision for its specific business and critical needs.

Supply and Technology Recovery

At this point, the BCP team has mapped out the necessary business functions that need to be up and running and the specific backup facility option that is best for its organization. Now the team needs to dig down into the more granular items, such as backup solutions for the following:

- Network and computer equipment
- Voice and data communications resources
- Human resources
- Transportation of equipment and personnel
- Environment issues (HVAC)
- Data and personnel security issues
- Supplies (paper, forms, cabling, and so on)
- Documentation

The organization’s current technical environment must be understood. This means the planners have to know the intimate details of the network, communications technologies, computers, network equipment, and software requirements that are necessary to get the critical functions up and running. What is surprising to some people is that many organizations do not totally understand how their network is configured and how it actually works, because the network was most likely established five to ten years ago and has kept growing like a teenage boy going through puberty. New devices are added, new computers are added, new software packages are added, VoIP may have been integrated, and the DMZ may have been split up into three DMZs, with an extranet for the company’s partners. Maybe the company bought and merged with another company and network. Over ten years, a number of technology refreshes most likely have taken place and the individuals who are maintaining the environment now are not the same people who built it ten years ago. Many IT departments experience employee turnover every one to five years. And most organizational network schematics are notoriously out of date, because everyone is busy with their current tasks or will come up with new tasks just to get out of having to update the schematic.

So the BCP team has to make sure that if the networked environment is partially or totally destroyed, the recovery team has the knowledge and skill to properly rebuild it.

NOTE Many organizations are moving to Voice over IP (VoIP), which means that if the network goes down, network and voice capability are unavailable. The team should address the possible need of redundant voice systems.

The BCP team needs to take into account several things that are commonly overlooked, such as hardware replacements, software products, documentation, environmental needs, and human resources.
Hardware Backups

*I have an extra floppy, video card, and some gum.*

Response: *I am sure that’s all we will need.*

The team has identified the equipment required to keep the critical functions up and running. This may include servers, user workstations, routers, switches, tape backup devices, hubs, and more. The needed inventory may seem simple enough, until the team drills down into more detail. If the recovery team is planning to use images to rebuild newly purchased servers and workstations (because the original ones were destroyed), will the images work on the new computers? Using images instead of building systems from scratch can be a time-saving task, unless the team finds out that the replacement equipment is a newer version and thus the images cannot be used. The BCP team should plan for the recovery team to use the company’s current images, but also have a manual process of how to build each critical system from scratch with the necessary configurations.

The BCP team also needs to identify how long it will take for new equipment to arrive. For example, if the organization has identified Gateway as its equipment replacement supplier, how long will it take this vendor to send 20 servers and 30 workstations to the offsite facility? After a disaster hits, the company could be in its offsite facility only to find that its equipment will take three weeks to be delivered. So, the SLA for the identified vendors needs to be investigated to make sure the company is not further damaged by delays. Once the parameters of the SLA are understood, the team must make a decision between depending upon the vendor or purchasing redundant systems and storing them as backups in case the primary equipment is destroyed. As described earlier, when potential company risks are identified, it is better to take preventive steps to reduce the potential damage. After the calculation of the MTD values, the team will know how long the company can be without a specific device. This data should be used to make the decision regarding whether the company should depend on the vendor’s SLA or make readily available a hot-swappable redundant system. If the company will lose $50,000 per hour if a particular server were to go down, then the team should elect to implement redundant systems and technology.

If an organization is using any legacy computers and hardware and a disaster hits tomorrow, where would it find replacements for this legacy equipment? The team should identify legacy devices and understand the risk the organization is under if replacements are unavailable. This type of finding has caused many companies to move from legacy systems to commercial off the shelf (COTS) products to ensure that replacement is possible.

**NOTE** Different types of backup tape technologies can be used (digital linear tape, digital audio tape, advanced intelligent tape). The team needs to make sure it knows the type of technology that is used by the company and identify the necessary vendor in case the tape-reading device needs to be replaced.

Software Backups

*I have a backup server and my backed-up data, but no operating system or applications.*

Response: *Good luck.*
Most companies’ IT departments have their array of software disks and licensing information here or there—or possibly in one centralized location. If the facility were destroyed and the IT department’s current environment had to be rebuilt, how would it gain access to these software packages? The BCP team should make sure to have an inventory of the necessary software required for mission-critical functions and have backup copies at an offsite facility. Hardware is usually not worth much to a company without the software required to run on it. The software that needs to be backed up can be in the form of applications, utilities, databases, and operating systems. The continuity plan must have provisions to back up and protect these items along with hardware and data.

The BCP team should make sure there are at least two copies of the company’s operating system software and critical applications. One copy should be stored onsite and the other copy should be stored at a secure offsite location. These copies should be tested periodically and re-created when new versions are rolled out.

It is common for organizations to work with software developers to create customized software programs. For example, in the banking world, individual financial institutions need software that will allow their bank tellers to interact with accounts, hold account information in databases and mainframes, provide online banking, carry out data replication, and perform a thousand other types of bank-like functionalities. This specialized type of software is developed and available through a handful of software vendors that specialize in this market. When bank A purchases this type of software for all of its branches, the software has to be specially customized for their environment and needs. Once this banking software is installed, the whole organization depends upon it for its minute-by-minute activities.

When bank A receives the specialized and customized banking software from the software vendor, bank A does not receive the source code. Instead, the software vendor provides bank A with a compiled version. Now, what if this software vendor goes out of business because of a disaster or bankruptcy? Then bank A will require a new vendor to maintain and update this banking software; thus, the new vendor will need access to the source code.

The protection mechanism that bank A should implement is called **software escrow**. Software escrow means that a third party holds the source code, backups of the compiled code, manuals, and other supporting materials. A contract between the software vendor, customer, and third party outlines who can do what and when with the source code. This contract usually states that the customer can have access to the source code only if and when the vendor goes out of business, is unable to carry out stated responsibilities, or is in breach of the original contract. If any of these activities takes place, then the customer is protected because it can still gain access to the source code and other materials through the third-party escrow agent.

Many companies have been crippled by not implementing software escrow. Such a company would have paid a software vendor to develop specialized software, and when the software vendor went belly up, the customer did not have access to the code that its whole company ran on.

The BCP committee needs to identify this issue as a vulnerability during its analysis and implement a preventive countermeasure—software escrow.
Documentation
We came up with a great plan six months ago. Did anyone write it down?

Documentation seems to be a dreaded task to most people, who will find many other tasks to take on to ensure they are not the ones stuck with documenting processes and procedures. However, a company may do a great and responsible job of backing up hardware and software to an offsite facility, maintaining it, and keeping everything up-to-date and current, but without documentation, when a disaster hits, no one will know how to put Humpty Dumpty back together again.

Restoration of files can be challenging, but restoring a whole environment that was swept away in a flood can be overwhelming, if not impossible. Procedures need to be documented because when they are actually needed, it will most likely be a chaotic and frantic atmosphere with a demanding time schedule. The documentation may need to include information on how to install images, configure operating systems and servers, and properly install utilities and proprietary software. Other documentation could include a calling tree, which outlines who should be contacted, in what order, and who is responsible for doing the calling. The documentation must also contain contact information for specific vendors, emergency agencies, offsite facilities, and any other entity that may need to be contacted in a time of need.

Most network environments evolve over time. Software has been installed on top of other software, configurations have been altered over the years to properly work in a unique environment, and service packs and patches have been installed to fix this problem or that issue. To expect one person or a group of people to go through all of these steps during a crisis and end up with an environment that looks and behaves exactly like the original environment and in which all components work together seamlessly may be a lofty dream.

So, the dreaded task of documentation may be the saving grace one day. It is an essential piece of business, and therefore an essential piece in disaster recovery and business continuity.

It is important to make one or more roles responsible for proper documentation. As with all the items addressed in this chapter, simply saying "All documentation will

Plans
Once the business continuity and disaster recovery plans are completed, where do you think they should be stored? Should the company have only one copy and keep it safely in a file cabinet next to Bob so that he feels safe? Nope. There should be two or three copies of these plans. One copy may be at the primary location, but the other copies should be at other locations in case the primary facility is destroyed. Typically, a copy is stored at the BCP coordinator’s home and another copy is stored at the offsite facility. This reduces the risk of not having access to the plans when needed.

These plans should not be stored in a file cabinet, but rather in a fire-resistant safe. When they are stored offsite, they need to be stored in a way that provides just as much protection as the primary site would provide.
be kept up-to-date and properly protected” is the easy part—saying and doing are two different things. Once the BCP team identifies tasks that must be done, the tasks must be assigned to individuals and those individuals have to be accountable. If these steps are not taken, the BCP team could have wasted a lot of time and resources defining these tasks, and the company could be in grave danger if a disaster occurs.

**NOTE**  
An organization may need to solidify communications channels and relationships with government officials and emergency response groups. The goal of this activity is to solidify proper protocol in case of a city- or region-wide disaster. During the BIA phase, local authorities should be contacted so the team understands the risks of its geographical location and how to access emergency zones. If the company has to initiate its BCP, many of these emergency response groups will need to be contacted during the recovery stage.

**Human Resources**

*We have everything up and running now—where are all the people to run these systems?*

One of the resources commonly left out of the equation is people. A company may restore its networks and critical systems and get business functions up and running, only to realize it doesn’t know the answer to the question, “Who will take it from here?” Human resources is a critical component to any recovery and continuity process, and it needs to be fully thought out and integrated into the plan.

What happens if we have to move to an offsite facility that is 250 miles away? We cannot expect people to drive back and forth from home to work. Should we pay for temporary housing for the necessary employees? Do we have to pay their moving costs? Do we need to hire new employees in the area of the offsite facility? If so, what skill set do we need from them? The BCP team should go through a long succession of these types of questions.

If a large disaster takes place that affects not only the company’s facility but also surrounding areas, including housing, do you think your employees will be more worried about your company or their families? Some companies assume that employees will be ready and available to help them get back into production, when in fact they may need to be at home because they have responsibilities to their families.

Regrettably, some employees may be killed in the disaster and the team may need to look at how it will be able to replace employees quickly through a temporary agency or a headhunter. This is extremely unfortunate, but it is part of reality. The team that identifies all threats and is responsible for identifying solutions needs to think about all of these issues and many more.

Organizations should already have **executive succession planning** in place. This means that if someone in a senior executive position retires, leaves the company, or is killed, the organization has predetermined steps to carry out to protect the company. The loss of a senior executive could tear a hole in the company’s fabric, creating a leadership vacuum that must be filled quickly with the right individual. The line of succession plan defines who would step in and assume responsibility for this role. Many organizations have “deputy” roles. For example, an organization may have a deputy CIO, deputy CFO, and deputy CEO ready to take over the necessary tasks if the CIO, CFO, or CEO becomes unavailable.
Often, larger organizations also have a policy indicating that two or more of the senior staff cannot be exposed to a particular risk at the same time. For example, the CEO and president cannot travel on the same plane. If the plane went down and both individuals were killed, then the company could be in danger. This is why you don’t see the President of the United States and the Vice President together too often. It is not because they don’t like each other and thus keep their distance from each other. It is because there is a policy indicating that to protect the United States, its top leaders cannot be under the same risk at the same time.

Reference


The End-User Environment

Do you think the users could just use an abacus for calculations and fire for light?

Because the end users are usually the worker bees of a company, they must be provided a functioning environment as soon as possible after a disaster hits. This means that the BCP team must understand the current operational and technical functioning environment and examine critical pieces so they can be replicated.

The first issue pertaining to users is how they will be notified of the disaster and who will tell them where to go and when. A tree structure of managers can be developed so that once a disaster hits, the person at the top of the tree calls two managers, and they in turn call three managers, and so on until all managers are notified. Each manager would be responsible for notifying the people he is responsible for until everyone is on the same page. Then, one or two people must be in charge of coordinating the issues pertaining to users. This could mean directing them to a new facility, making sure they have the necessary resources to complete their tasks, restoring data, and being a liaison between the different groups. The folks in charge of directing should be readily identifiable—by wearing an emergency hat and vest, for example—and should be located in areas where they can be seen by all. This will help ease confusion and reduce panic during difficult and strenuous times.

In most situations, after a disaster, only a skeleton crew is put back to work. The BCP committee identified the most critical functions of the company during the analysis stage, and the employees who carry out those functions must be put back to work first. So the recovery process for the user environment should be laid out in different stages. The first stage is to get the most critical departments back online, the next stage is to get the second most important back online, and so on.

The BCP team needs to identify user requirements, such as whether users can work on stand-alone PCs or need to be connected in a network to fulfill specific tasks. For example, in a financial institution, users who work on stand-alone PCs might be able to accomplish some small tasks like filling out account forms, word processing, and accounting tasks, but they would need to be connected to a host system to update customer profiles and to interact with the database.

The BCP team also needs to identify how current automated tasks can be carried out manually if that becomes necessary. If the network is going to be down for 12 hours,
could the necessary tasks be carried out through traditional pen and paper methods? If the Internet connection is going to be down for five hours, could the necessary communications take place through phone calls? Instead of transmitting data through the internal mail system, could couriers be used to run information back and forth? Today, we are extremely dependent upon technology, but we often take for granted that it will always be there for us to use. It is up to the BCP team to realize that technology may be unavailable for a period of time and come up with solutions for those situations.

### Data Backup Alternatives

As we have discussed so far, backup alternatives are needed for hardware, software, personnel, and offsite facilities. It is up to each company and its continuity team to decide if all of these components are necessary for its survival and the specifics for each type of backup needed.

Data have become one of the most critical assets to nearly all organizations. These data may include financial spreadsheets, blueprints on new products, customer information, product inventory, trade secrets, and more. In Chapter 3, we stepped through risk analysis procedures and data classification processes. The BCP team should not be responsible for setting up and maintaining the company’s data classification procedures, but the team may recognize that the company is at risk because it does not have these procedures in place. This should be seen as a vulnerability that is reported to management. Management would need to establish another group of individuals who would identify the company’s data, define a loss criterion, and establish the classification structure and processes.

The BCP team’s responsibility is to provide solutions to protect this data and identify ways to restore it after a disaster. In this section, we look at different ways data can be protected and restored when needed.

Data usually change more often than hardware and software, so these backup procedures must happen on a continual basis. The data backup process must make sense and be reasonable and effective. If data in the files change several times a day, backup procedures should happen a few times a day or nightly to ensure all the changes are captured and kept. If data are changed once a month, backing up data every night is a waste of time and resources. Backing up a file and its corresponding changes is usually more desirable than having multiple copies of that one file. Online backup technologies usually have the changes to a file made to a transaction log, which is separate from the original file.

The operations team is responsible for defining which data get backed up and how often. These backups can be full, differential, or incremental backups and are usually used in some type of combination with each other. Most files are not altered every day, so, to save time and resources, it is best to devise a backup plan that does not continually back up data that has not been modified. So, how do we know which data have changed and need to be backed up without having to look at every file’s modification date? This is accomplished by an archive bit. Operating systems’ file systems keep track of what files have been modified by setting an archive bit. If a file is modified or created, the file system sets the archive bit to 1. Backup software has been created to review this bit setting when making its determination on what gets backed up and what does not.
The first step is to do a full backup, which is just what it sounds like—all data are backed up and saved to some type of storage media. During a full backup, the archive bit is clear, which means that it is set to 0. A company can choose to do full backups only, in which case the restoration process is just one step, but the backup and restore processes could take a long time.

Most companies choose to combine a full backup with a differential or incremental backup. A differential process backs up the files that have been modified since the last full backup. When the data need to be restored, the full backup is laid down first and then the differential backup is put down on top of it. The differential process does not change the archive bit value.

An incremental process backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0. When the data need to be restored, the full backup data are laid down and then each incremental backup is laid down on top of it in the proper order (see Figure 9-2). If a company experienced a disaster and it used the incremental process, it would first need to restore the full backup on its hard drives and lay down every incremental backup that was carried out before the disaster took place. So, if the full backup was done six months ago and the operations department carried out an incremental backup each month, the restoration team would restore the full backup and start with the older incremental backups and restore each one of them until they were all restored.

Which backup process is best? If a company wants the backup and restoration processes to be simplistic and straightforward, it can carry out just full backups—but this may require a lot of hard drive space and time. Although using differential and incremental backup processes is more complex, it requires less resources and time. A differential backup takes more time in the backing up phase than an incremental backup, but it also takes less time to restore than an incremental backup, because carrying out restoration of a differential backup happens in two steps, whereas in an incremental backup every incremental backup must be restored in the correct sequence.

**Figure 9-2**
Backup software may alter the archive bit.
Whatever the organization chooses, it is important to not mix differential and incremental backups. This overlap could cause files to be missed, since the incremental backup changes the archive bit and the differential backup does not.

Critical data should be backed up and stored at an onsite area and an offsite area. The onsite backup copies should be easily accessible in case of non-disasters and should provide a quick restore process so operations can return to normal. However, onsite backup copies are not enough to provide real protection. The data should also be held in an offsite facility in case of actual disasters or catastrophes. One choice that needs to be made is where the offsite location should be in reference to the main facility. The closer the offsite backup storage site is, the easier it is to access, but this can put the backup copies in danger if a large-scale disaster manages to take out the company’s main facility and the backup facility. It may be wiser to choose a backup facility farther away, which makes accessibility harder but reduces the risk. Some companies choose to have more than one backup facility: one that is close and one that is farther away.

The onsite backup information should be stored in a fire-resistant, heat-resistant, and waterproof safe. The procedures for backing up and restoring data should be easily accessible and comprehensible even to operators or administrators who are not intimately familiar with a specific system. In an emergency situation, the same guy who always does the backing up and restoring may not be around, or outsourced consultants may need to be temporarily hired in order to meet the restoration time constraints.

A backup strategy must take into account that failure can take place at any step of the process, so if there is a problem during the backup or restoration process that could corrupt the data, there should be a graceful way of backing out or reconstructing the data from the beginning.

Can we actually restore data? Backing up data is a wonderful thing in life, but making sure it can be properly restored is even better. Many organizations have developed a false sense of security based on the fact that they have a very organized and effective process of backing up their data. That sense of security can disappear in seconds when a company realizes in a time of crisis that its restore processes do not work. For example, one company had paid an offsite backup facility to use a courier to collect its weekly backup tapes and transport them to the offsite facility for safekeeping. What the company did not realize was that this courier used the subway and many times set the tapes on the ground while waiting for the subway train. A subway has many large engines that create their own magnetic field. This can have the same effect on media as large magnets, meaning that the data can be erased or corrupted. The company never tested its restore processes and eventually experienced a disaster. Much to its surprise, it found out that three years of data was corrupted and unusable.

Many other stories and experiences like this are out there. Don’t let your organization end up as an anecdote in someone else’s book because it failed to verify that its backups can be restored.

**Electronic Backup Solutions**

Manually backing up systems and data can be time-consuming, error prone, and costly. Several technologies serve as automated backup alternatives. Although these technologies are usually more expensive, they are quicker and more accurate, which may be necessary for online information that changes often.
Among the many technologies and ways to back up data electronically is **disk shadowing**, which is very similar to data mirroring.

**NOTE**  
*Disk duplexing* means there is more than one disk controller. If one disk controller fails, the other is ready and available.

Disk shadowing is used to ensure the availability of data and provide a fault-tolerant solution by duplicating hardware and maintaining more than one copy of the information. The data are dynamically created and maintained on two or more identical disks. If only disk mirroring is used, then each disk would have a corresponding mirrored disk that contains the exact same information. If shadow sets are used, the data can be stored as images on two or more disks.

Systems that need to interact with this data are connected to all the drives at the same time. All of these drives “look” like just one drive to the user. This provides transparency to the user so that when she needs to retrieve a file, she does not have to worry about which drive to go to for this process. When a user writes data to be stored on this media, the data are written to all disks in the shadow set.

Disk shadowing provides online backup storage, which can either reduce or replace the need for periodic offline manual backup operations. Another benefit to this solution is that it can boost read operation performance. Multiple paths are provided to duplicate data, and a shadow set can carry out multiple read requests in parallel.

Disk shadowing is commonly seen as an expensive solution, because two or more hard drives are used to hold the exact same data. If a company has data that will fill up 100 hard drives, it must purchase and maintain at least 200 hard drives. A company would choose this solution if fault tolerance were required.

If a disk drive fails, at least one shadow set is still available. A new disk can be assigned to this set through proper configurations, and the data can be copied from the shadow set. The copying can take place offline, but this means the data are unavailable for a period of time. Most products that provide disk-shadowing functionality allow for online copying, where disks are hot swapped into the set and can carry out the necessary copy functions without having to bring the drives offline.

Electronic vaulting and remote journaling are other solutions that companies should be aware of. **Electronic vaulting** makes copies of files as they are modified and periodically transmits them to an offsite backup site. The transmission does not happen in real time, but is carried out in batches. So, a company can choose to have all files that have been changed sent to the backup facility every hour, day, week, or month. The information can be stored in an offsite facility and retrieved from that facility in a short period of time.

This form of backup takes place in many financial institutions, so when a bank teller accepts a deposit or withdrawal, the change to the customer’s account is made locally to that branch’s database and to the remote site that maintains the backup copies of all customer records.
Electronic vaulting is a method of transferring bulk information to offsite facilities for backup purposes. Remote journaling is another method of transmitting data offsite, but this usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data are corrupted and need to be restored, the bank can retrieve these logs, which are used to rebuild the lost data. Journaling is efficient for database recovery, where only the reapplication of a series of changes to individual records is required to resynchronize the database.

NOTE  Remote journaling takes place in real time and transmits only the file deltas. Electronic vaulting takes place in batches and moves the entire file that has been updated.

It may be necessary to keep different versions of software and files, especially in a software development environment. The object and source code should be backed up along with libraries, patches, and fixes. The offsite facility should mirror the onsite facility, meaning it does not make sense to keep all of this data at the onsite facility and only the source code at the offsite facility. Each site should have a full set of the most current and updated information and files.

Another software backup technology we will discuss is referred to as tape vaulting. Many businesses back up their data to tapes that are then manually transferred to an offsite facility by a courier or an employee. With automatic tape vaulting, the data are sent over a serial line to a backup tape system at the offsite facility. The company that maintains the offsite facility maintains the systems and changes out tapes when necessary. Data can be quickly backed up and retrieved when necessary. This technology reduces the manual steps in the traditional tape backup procedures.

Basic vaulting of tape data is sending backup tapes to an offsite location, but a manual process can be error prone. Electronic tape vaulting transmits data over a net-
work to tape devices located at an alternate data center. Electronic tape vaulting improves recovery speed and reduces errors, and backups can be run more frequently.

Choosing a Software Backup Facility

I like this facility because it is pink.

A company needs to address several issues and ask specific questions when it is deciding upon a storage facility for its backup materials. The following provides a list of just some of the issues that need to be thought through before committing to a specific vendor for this service:

- Can the media be accessed in the necessary timeframe?
- Is the facility closed on weekends and holidays, and does it only operate during specific hours of the day?
- Are the access control mechanisms tied to an alarm and/or the police station?
- Does the facility have the capability to protect the media from a variety of threats?
- What is the availability of a bonded transport service?
- Are there any geographical environmental hazards such as floods, earthquakes, tornadoes, and so on?
- Is there a fire detection and suppression system?
- Does the facility provide temperature and humidity monitoring and control?
- What type of physical, administrative, and logical access controls are used?

The questions and issues that need to be addressed will vary depending on the type of company, its needs, and the requirements of a backup facility.
Which Data Recovery Solution?
Data classification based on business criticality should have been performed by now.

- The BCP project team needs to divide the data by importance of fast recovery.
- Critical data that need to be continuously available can be restored via electronic vaulting (or remote journaling).
- Other data types can be restored via tapes or mirror systems.

Asynchronous replication means the primary and secondary data volumes are only a few milliseconds out of sync, so the replication is nearly real-time. With synchronous replication, the primary and secondary copies are always identical, which provides true real-time duplication. Synchronous means replication does not take place in real time, such as in electronic vaulting or batch jobs.
The team must balance the cost to recover against the cost of the disruption. The balancing point becomes the recovery time objective.

Insurance

*Can someone else just pay for this mess?*

*Response: Sure, we just need a monthly fee.*

During the BIA, the team most likely uncovered several threats that the organization could not prevent. Taking on the full risk of these threats often is dangerous, which is why insurance exists. The decision of whether or not to obtain insurance for a particular threat, and how much coverage to obtain when choosing to insure, should be based on the probability of the threat becoming real and the loss potential, which was identified during the BIA. The BCP team should work with management to understand what the current coverage is, the various insurance options, and the limits of each option. The goal here is to make sure the insurance coverage fills in the gap of what the current preventive countermeasures cannot protect against. We can eat healthy, work out, and take our vitamins—but these things cannot prevent death. We purchase life insurance so that after we die, our loved ones are taken care of. (Seems more appropriate to call this death insurance, but that would really hurt marketing efforts of insurance companies.)
Just as people are given different premiums on health and life insurance, companies are given different premiums on the type of insurance they purchase. Different types of insurance policies can be purchased by companies, cyberinsurance being one of them. Cyberinsurance is a new type of coverage that insures losses caused by Denial-of-Service attacks, malware damages, hackers, electronic theft, privacy-related lawsuits, and more. While a person is asked how old he is, previous health issues, if he smokes, and so on to determine his health insurance premium, companies are asked questions about their security program, such as whether they have an IDS, antivirus software, firewalls, and other security measures.

A company could also choose to purchase a business interruption insurance policy. With this type of policy, if the company is out of business for a certain length of time, the insurance company will pay for specified expenses and lost earnings. Another policy that can be bought insures accounts receivable. If a company cannot collect on its accounts receivable for one reason or another, this type of coverage covers part or all of the losses and costs.

The company's insurance should be reviewed annually, because threat levels may change and the company may expand into new ventures that need to be properly covered. Purchasing insurance should not lull a company into a false sense of security, though. Insurance coverage has its limitations, and if the company does not practice due care, the insurance company may not be legally obligated to pay if a disaster hits. It is important to read and understand the fine print when it comes to insurance and make sure you know what is expected of your company—not just what is expected from the insurance organization.

**Recovery and Restoration**

*Now, who is going to fix everything?*

*Response: We thought you were.*

The BCP coordinator needs to define several different teams that should be properly trained and available if a disaster hits. The types of teams an organization needs depends upon the organization. The following are some examples of teams that a company may need to construct:

- Damage assessment team
- Legal team
- Media relations team
- Network recovery team
- Relocation team
- Restoration team
- Salvage team
- Security team
- Telecommunications team
The BCP coordinator should have an understanding of the needs of the company and the types of teams that need to be developed and trained. Employees should be assigned to the specific teams based on their knowledge and skill set. Each team needs to have a designated leader, who will direct the members and their activities. These team leaders will be responsible not only for ensuring that their team’s objectives are met, but also for communicating with each other to make sure each team is working in parallel phases.

The *restoration team* should be responsible for getting the alternate site into a working and functioning environment, and the *salvage team* should be responsible for starting the recovery of the original site. Both teams must know how to do many tasks, such as install operating systems, configure workstations and servers, string wire and cabling, set up the network and configure networking services, and install equipment and applications. Both teams must also know how to restore data from backup facilities, and how to do so in a secure manner that ensures the system’s and data’s confidentiality, integrity, and availability are not compromised.

The BCP must outline the specific teams, their responsibilities, and notification procedures. The plan must indicate the methods that should be used to contact team leaders during business hours and after business hours.

A role, or a team, needs to be created to carry out a *damage assessment* once a disaster has taken place. The assessment procedures should be properly documented and include the following steps:

- Determine the cause of the disaster.
- Determine the potential for further damage.
- Identify the affected business functions and areas.
- Identify the level of functionality for the critical resources.
- Identify the resources that must be replaced immediately.
- Estimate how long it will take to bring critical functions back online.
- If it will take longer than the previously estimated MTD values to restore operations, then a disaster should be declared and the BCP should be put into action.

After this information is collected and assessed, it will indicate what teams need to be called to action and whether the BCP actually needs to be activated. The BCP coordinator and team must develop activation criteria. After the damage assessment, if one or more of the situations outlined in the criteria have taken place, then the team is moved into recovery mode.

Different organizations have different criteria, because the business drivers and critical functions will vary from organization to organization. The criteria may comprise some or all of the following elements:

- Danger to human life
- Danger to state or national security
- Damage to facility
- Damage to critical systems
- Estimated value of downtime that will be experienced
Once the damage assessment is completed and the plan is activated, various teams must be deployed, which signals the company’s entry into the recovery phase. Each team has its own tasks—for example, the restoration team prepares the offsite facility (if needed), the network team rebuilds the network and systems, and the relocation team starts organizing the staff to move into a new facility.

The recovery process needs to be as organized as possible to get the company up and running as soon as possible. This is much easier to state in a book than to carry out in reality. This is why written procedures are critical. During the BIA, the critical functions and their resources were identified. These are the things that the teams need to work together on getting up and running first. Templates should be developed during the plan development stage. These templates are used by the different teams to step them through the necessary phases and to document their findings. For example, if one step could not be completed until new systems were purchased, this should be indicated on the template. If a step is partially completed, this should be documented so the team does not forget to go back and finish that step when the necessary part arrives. These templates keep the teams on task and also quickly tell the team leaders about the progress, obstacles, and potential recovery time.

**NOTE** Examples of possible templates can be found in NIST’s *Contingency Planning Guide for Information Technology Systems*, which is available online at http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

When it is time for the company to move back into its original site or a new site, the company is ready to enter into the reconstitution phase. A company is not out of an emergency state until it is back in operation at the original primary site or a new site that was constructed to replace the primary site, because the company is always vulnerable while operating in a backup facility. Many logistical issues need to be considered as to when a company must return from the alternate site to the original site. The following lists a few of these issues:

- Ensuring the safety of employees
- Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC)
- Ensuring that the necessary equipment and supplies are present and in working order
- Ensuring proper communications and connectivity methods are working
- Properly testing the new environment

Once the coordinator, management, and salvage team sign off on the readiness of the facility, the salvage team should carry out the following steps:

- Back up data from the alternate site and restore it within the new facility
- Carefully terminate contingency operations
- Securely transport equipment and personnel to the new facility
The least critical functions should be moved back first, so if there are issues in network configurations or connectivity, or important steps were not carried out, the critical operations of the company are not negatively affected. Why go through the trouble of moving the most critical systems and operations to a safe and stable site, only to return it to a main site that is untested? Let the less critical departments act as the canary. If they survive, then move over the more critical components of the company.

Up to now, the BCP team has covered the following steps:

1. Developed the continuity planning policy statement
   - Outlined the scope and goals of the BCP and roles of the BCP team
2. Performed the business impact analysis (BIA)
   - Identified critical business functions, their resources, and MTD values
   - Identified threats and calculated the impact of these threats
   - Identified solutions
   - Presented findings to management
3. Identified and implemented preventive controls

- Put controls into place to reduce the company’s identified risks
- Bought more insurance, implemented facility structural reinforcements, rolled out backup solutions for data, installed redundant and fault-tolerant mechanisms, and so on

4. Developed recovery strategies

- Implemented processes of getting the company up and running in the necessary time
- Created the necessary teams, developed goals and procedures for each team, created notification steps and planned activation criteria, identified alternate backup solutions, and so on

So, the BCP team has worked long and hard and has all of the previous items figured out. Now it needs to put all of these solutions and steps in the plan itself, test the plan, train the people, and lay out strategies of how the plan is to be maintained and kept up-to-date. No rest for the weary…let’s march on!

References

- Business Continuity Planning & Disaster Recovery Planning Directory, Disaster Recovery World www.disasterrecoveryworld.com

BCP Development Products

Since there is so much work in collecting analyzing and maintaining DRP and BCP data, using a product that automates these tasks can prove to be extremely helpful. “Automated” plan development can help you create:

- Customizable questionnaires through the use of expert-system templates
- Timetables for disaster recovery procedures
- What-if scenario modeling
- Reports on financial and operational impact analysis
- Graphic representations of the analysis results
- Sample questionnaires, forms, and templates
- Permission-based plan maintenance
- Central version control and integration
- Regulatory compliance
Developing Goals for the Plans

My goals are to own a boat, retire at 55, and grow more hair.
Response: Great, we will integrate this into our BCP.

If you do not have established goals, how do you know when you are done and whether your efforts were actually successful? Goals are established so everyone knows the ultimate objectives. Establishing goals is important for any task, but especially for business continuity and recovery plans. The definition of the goals helps direct the proper allocation of resources and tasks, develops necessary strategies, and assists in economical justification of the plans and program overall. Once the goals are set, they provide a guide to the development of the actual plans themselves. Anyone who has been involved in large projects that entail many small, complex details knows that at times it is easy to get off track and not actually accomplish the major goals of the project. Goals are established to keep everyone on track and ensure that the efforts pay off in the end.

Great, we have established that goals are important. But the goal could be, “Keep the company in business if an earthquake hits.” Good goal, but not overly useful without more clarity and direction. To be useful, a goal must contain certain key information, such as the following:

- **Responsibility** Each individual involved with recovery and continuity should have their responsibilities spelled out in writing to ensure a clear understanding in a chaotic situation. Each task should be assigned to the individual most logically situated to handle it. These individuals must know what is expected of them, which is done through training, drills, communication, and documentation. So, for example, instead of just running out of the building screaming, an individual must know that he is responsible for shutting down the servers before he can run out of the building screaming.

- **Authority** In times of crisis, it is important to know who is in charge. Teamwork is important in these situations, and almost every team does much better with an established and trusted leader. Such leaders must know that they are expected to step up to the plate in a time of crisis and understand what type of direction they should provide to the rest of the employees. Clear-cut authority will aid in reducing confusion and increasing cooperation.

- **Priorities** It is extremely important to know what is critical versus what is merely nice to have. Different departments provide different functionality for an organization. The critical departments must be singled out from the departments that provide functionality that the company can live without for a week or two. It is necessary to know which department must come online first, which second, and so on. That way, the efforts are made in the most useful, effective, and focused manner. Along with the priorities of departments, the priorities of systems, information, and programs must be established. It may be necessary to ensure that the database is up and running before working to bring the file server online. The general priorities must be set by the management with the help of the different departments and IT staff.
Implementation and testing It is great to write down very profound ideas and develop plans, but unless they are actually carried out and tested, they may not add up to a hill of beans. Once a continuity plan is developed, it actually has to be put into action. It needs to be documented and put in places that are easily accessible in times of crisis. The people who are assigned specific tasks need to be taught and informed how to fulfill those tasks, and dry runs must be done to walk people through different situations. The drills should take place at least once a year, and the entire program should be continually updated and improved.

Studies have shown that 65 percent of businesses that lose computing capabilities for over one week are never able to recover, and subsequently go out of business. Not being able to bounce back quickly or effectively by setting up shop somewhere else can make a company lose business and, more importantly, its reputation. In such a competitive world, customers have a lot of options. If one company is not prepared to bounce back after a disruption or disaster, customers may go to another vendor and stay there.

Implementing Strategies

Once the strategies have been decided upon, they need to be documented and put into place by the BCP team. This moves the efforts from a purely planning stage to an actual implementation and action phase.

As stated previously, copies of the plans need to be kept in one or more locations other than the primary site, so that if the primary site is destroyed or negatively affected, the continuity plan is still available to the teams. It is also critical that different formats of the plan be available to the team, including both electronic and paper versions. An electronic version of the plan is not very useful if you don’t have any electricity to run a computer. In addition to having copies of the recovery documents located at their offices and homes, key individuals should also have easily accessible versions of critical procedures and call tree information. One simple way to accomplish this is to publish the call tree data on cards that can be affixed to personnel badges or kept in a wallet. In an emergency situation, valuable minutes are better spent responding to an incident than looking for a document or having to wait for a laptop to power up.

The plan should address in detail all of the topics we have covered so far. The actual format of the plan will depend on the environment, the goals of the plan, priorities, and identified threats. After each of those items is examined and documented, the topics of the plan can be divided into the necessary categories.

A commonly accepted structure for a BCP is illustrated in Figure 9-3. Each organization’s BCP looks different, but these core topics should be covered in some fashion. We walked through these different components earlier in this chapter. The role of the plan is to provide preplanned and sequenced structure to these different processes. The plan also needs to integrate a degree of flexibility, because no one knows exactly what type of disaster will take place, nor its effects. Although procedures need to be documented for the different phases of the plan, a balance between detail and flexibility must be achieved so the company is not ready for only one type of disaster.
Some organizations develop individual plans for specific tasks and goals. These different plans are described in Table 9-2. It is up to management and the BCP team to determine the number and types of plans that should be developed and implemented. The BCP team can choose to integrate many of these components into the BCP. It is usually better to include these stand-alone plans as appendices so each document is clear, concise, and useable.

**Testing and Revising the Plan**

*We made a plan and tested it and it doesn’t work.*

*Response: Let’s just go home then.*

The BCP should be tested regularly, because environments continually change. Interestingly, many organizations are moving away from the concept of “testing” because a test naturally leads to a pass or fail score, and in the end, that type of score is not very productive. Instead, many organizations are adopting the concept of exercises, which

---

**Figure 9-3**

The general structure of a business continuity plan

<table>
<thead>
<tr>
<th>Section</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Initiation</td>
<td>- Goal statement</td>
</tr>
<tr>
<td></td>
<td>- Overview of concepts</td>
</tr>
<tr>
<td></td>
<td>- Roles and teams definitions</td>
</tr>
<tr>
<td></td>
<td>- Task definitions</td>
</tr>
<tr>
<td>II. Activation</td>
<td>- Notification steps</td>
</tr>
<tr>
<td></td>
<td>- Damage assessment</td>
</tr>
<tr>
<td></td>
<td>- Plan activation</td>
</tr>
<tr>
<td>III. Recovery</td>
<td>- Move to alternate site</td>
</tr>
<tr>
<td></td>
<td>- Restore processes</td>
</tr>
<tr>
<td></td>
<td>- Recovery procedures</td>
</tr>
<tr>
<td>IV. Reconstruction</td>
<td>- Restore facility</td>
</tr>
<tr>
<td></td>
<td>- Test environment</td>
</tr>
<tr>
<td></td>
<td>- Move operations</td>
</tr>
<tr>
<td>V. Appendixes</td>
<td>- Calling tree data</td>
</tr>
<tr>
<td></td>
<td>- Other plan types</td>
</tr>
<tr>
<td></td>
<td>- Schematics</td>
</tr>
<tr>
<td></td>
<td>- System requirements</td>
</tr>
</tbody>
</table>
appear to be less stressful, better focused, and ultimately more productive. Each time
the plan is exercised or tested, improvements and efficiencies are generally uncovered,
yielding better and better results over time. The responsibility of establishing periodic
exercises and the maintenance of the plan should be assigned to a specific person or
persons who will have overall ownership responsibilities for the business continuity
initiatives within the organization.

As noted earlier, the plan’s maintenance should be incorporated into change man-
agement procedures so any changes in the environment are reflected in the plan itself.

Tests and disaster recovery drills and exercises should be performed at least once a
year. A company should have no real confidence in a developed plan until it has actually
been tested. The tests and drills prepare personnel for what they may be faced with and
provide a controlled environment to learn the tasks expected of them. These tests and
drills also point out issues to the planning team and management that may not have
been previously thought about and addressed as part of the planning process. The exer-
cises, in the end, demonstrate whether a company can actually recover after a disaster.

<table>
<thead>
<tr>
<th>Plan Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business resumption plan</td>
<td>Focuses on how to re-create the necessary business processes that need to be reestablished instead of focusing on IT components (i.e., process-oriented instead of procedural-oriented).</td>
</tr>
<tr>
<td>Continuity of operations plan (COOP)</td>
<td>Establishes senior management and a headquarters after a disaster. Outlines roles and authorities, orders of succession, and individual role tasks.</td>
</tr>
<tr>
<td>IT contingency plan</td>
<td>Plan for systems, networks, and major applications recovery procedures after disruptions. A contingency plan should be developed for each major system and application.</td>
</tr>
<tr>
<td>Crisis communications plan</td>
<td>Includes internal and external communications structure and roles. Identifies specific individuals who will communicate with external entities. Contains predeveloped statements that are to be released.</td>
</tr>
<tr>
<td>Cyber incident response plan</td>
<td>Focuses on malware, hackers, intrusions, attacks, and other security issues. Outlines procedures for incident response.</td>
</tr>
<tr>
<td>Disaster recovery plan</td>
<td>Focuses on how to recover various IT mechanisms after a disaster. Whereas a contingency plan is usually for nondisasters, a disaster recovery plan is for disasters that require IT processing to take place at another facility.</td>
</tr>
<tr>
<td>Occupant emergency plan</td>
<td>Establishes personnel safety and evacuation procedures.</td>
</tr>
</tbody>
</table>

Table 9-2 Different Types of Recovery Plans
The exercise should have a predetermined scenario that the company may indeed be faced with one day. Specific parameters and a scope of the exercise must be worked out before sounding the alarms. The team of testers must agree upon what exactly is getting tested and how to properly determine success or failure. The team must agree upon the timing and duration of the exercise, who will participate in the exercise, who will receive which assignments, and what steps should be taken. Also, the team needs to determine whether hardware, software, personnel, procedures, and communications lines are going to be tested, and whether it is some, all, or a subset combination. If the test will include moving some equipment to an alternate site, then transportation, extra equipment, and alternate site readiness must be addressed and assessed.

Most companies cannot afford for these exercises to interrupt production or productivity, so the exercises may need to take place in sections or at specific times, which will require logistical planning. Written exercise plans should be developed that will test for specific weaknesses in the overall disaster recovery plan. The first exercise should not include all employees, but rather a small group of people here and there until each learns his or her responsibilities. Then, larger drills can take place so overall operations will not be negatively affected. The people carrying out these drills should expect problems and mistakes. This is why they are having the drills in the first place. A company would rather have employees make mistakes during a drill so they can learn from them and perform their tasks more effectively during a real disaster.

NOTE
After a disaster, telephone service may not be available. For communications purposes, there should be alternatives in place, such as cell phones or walkie-talkies.

A few different types of drills and tests can be used, each with its own pros and cons. The following sections explain the different types of drills.

**Checklist Test**
*Okay, did we forget anything?*

In this type of test, copies of the BCP are distributed to the different departments and functional areas for review. This is done so each functional manager can review the plan and indicate if anything has been left out or if some approaches should be modified or deleted. This is a method that ensures that some things have not been taken for granted or omitted. Once the departments have reviewed their copies and made suggestions, the planning team then integrates those changes into the master plan.

**Structured Walk-Through Test**
*Let’s get in a room and talk about this.*

In this test, representatives from each department or functional area come together to go over the plan to ensure its accuracy. The group reviews the objectives of the plan, discusses the scope and assumptions of the plan, reviews the organization and reporting structure, and evaluates the testing, maintenance, and training requirements described. This gives the people responsible for making sure a disaster recovery happens
effectively and efficiently a chance to review what has been decided upon and what is expected of them.

The group walks through different scenarios of the plan from beginning to end to make sure nothing was left out. This also raises the awareness of the recovery procedures to team members.

**Simulation Test**

*Everyone take your places. Okay, action!*  

This type of test takes a lot more planning and people. In this situation, all employees who participate in operational and support functions, or their representatives, come together to practice executing the disaster recovery plan based on a specific scenario. The scenario is used to test the reaction of each operational and support representative. Again, this is done to ensure specific steps were not left out and certain threats were not overlooked. It acts as a catalyst to raise the awareness of the people involved.

The drill includes only those materials that will be available in an actual disaster, to portray a more realistic environment. The simulation test continues up to the point of actual relocation to an offsite facility and actual shipment of replacement equipment.

**Parallel Test**

*Let’s do a little processing here and a little processing there.*  

A parallel test is done to ensure that the specific systems can actually perform adequately at the alternate offsite facility. Some systems are moved to the alternate site and processing takes place. The results are compared with the regular processing that is done at the original site. This points out any necessary tweaking, reconfiguring, or steps that need to take place.

**Full-Interruption Test**

*Shut down and move out!*  

This type of test is the most intrusive to regular operations and business productivity. The original site is actually shut down and processing takes place at the alternate site. The recovery team fulfills its obligations in preparing the systems and environment for the alternate site. All processing is done only on devices at the alternate offsite facility.

This is a full-blown drill that takes a lot of planning and coordination, but it can reveal many holes in the plan that need to be fixed before an actual disaster hits. Full-interruption tests should be performed only after all other types of tests have been successful. They are the most risky and can impact the business in very serious and devastating ways if not managed properly; therefore, senior management approval needs to be obtained prior to performing full-interruption tests.

The type of organization and its goals will dictate what approach to the training exercise is most effective. Each organization may have a different approach and unique aspects. If detailed planning methods and processes are going to be taught, then specific training may be required, rather than general training that provides an overview. Higher-quality training will result in an increase of employee interest and commitment.

During and after each type of test, a record of the significant events should be documented and reported to management so it is aware of all outcomes of the test.
Other Types of Training

*I think I stopped breathing. Quick, blow into my mouth!*

*Response: Leave me alone.*

Employees need to be trained on other issues besides disaster recovery, including first aid and CPR, how to properly use a fire extinguisher, evacuation routes and crowd control methods, emergency communications procedures, and how to properly shut down equipment in different types of disasters.

The more technical employees may need to know how to redistribute network resources and use different telecommunications lines if the main one goes down. A redundant power supply needs to be investigated, and the procedures for how to move critical systems from one power supply to the next should be understood and tested.

Emergency Response

*You must save your fellow man before any equipment.*

*Response: But I love my computer more than anyone I know.*

Often, the initial response to an emergency affects the ultimate outcome. Emergency response procedures are the prepared actions that are developed to help people in a crisis situation better cope with the disruption. These procedures are the first line of defense when dealing with a crisis situation.

People who are up-to-date on their knowledge of disaster recovery will perform the best, which is why training and drills are very important. Emergencies are unpredictable, and no one knows when they will be called upon to perform.

Protection of life is of the utmost importance and should be dealt with first before looking to save material objects. Training and drills should show the people in charge how to evacuate personnel safely (see Table 9-3). All personnel should know their designated emergency exits and destinations. Emergency gathering spots should take into consideration the effects of seasonal weather. One person in each designated group is often responsible for making sure all people are accounted for. One person in particular should be responsible for notifying the appropriate authorities: the police department, security guards, fire department, emergency rescue, and management. With proper training, employees will be better equipped to handle emergencies rather than just running to the exit.

If the situation is not life threatening, systems should be shut down in an orderly fashion, and critical data files or resources, along with critical personal items like purses and wallets, should be removed during evacuation. There is a reason for the order of activities. As with all processes, there are dependencies with everything we do. Deciding to skip steps or add steps could in fact cause more harm than good.

Once things have approached a reasonable plateau of activity, one or more people will most likely be required to interface with external entities, such as the press, customers, shareholders, and civic officials. One or more people should be prepped in their reaction and response to the recent disaster so a uniform and reasonable response is given to explain the circumstances, how the company is dealing with the disaster, and what customers and others should now expect from the company. The company should quickly present this information instead of having others come to their own conclu-
sions and start false rumors. At least one person should be available to the press to ensure proper messages are being reported and sent out.

Another, unfortunate issue needs to be addressed prior to an emergency: potential looting, vandalism, and fraud opportunities from both a physical and logical perspective. After a company is hit with a large disturbance or disaster is usually when it is most vulnerable, and others may take advantage of this vulnerability. Careful thought and planning needs to take place so these issues can be dealt with properly and the necessary and expected level of protection is provided at all times.

**Maintaining the Plan**

*Wow, this plan was developed in 1958!*

*Response: I am sure it is still fine. Not much has changed since then.*

Unfortunately, the various plans that have been covered in this chapter can become quickly out of date. An out-of-date BCP may provide a company with a false sense of security, which could be devastating if and when a disaster actually takes place.
The main reasons plans become outdated include the following:

- The business continuity process is not integrated into the change management process.
- Infrastructure and environment changes occur.
- Reorganization of the company, layoffs, or mergers occur.
- Changes in hardware, software, and applications occur.
- After the plan is constructed, people feel their job is done.
- Personnel turns over.
- Large plans take a lot of work to maintain.
- Plans do not have a direct line to profitability.

Organizations can keep the plan updated by taking the following actions:

- Make business continuity a part of every business decision.
- Insert the maintenance responsibilities into job descriptions.
- Include maintenance in personnel evaluations.
- Perform internal audits that include disaster recovery and continuity documentation and procedures.
- Perform regular drills that use the plan.
- Integrate the BCP into the current change management process.

One of the simplest and most cost-effective and process-efficient ways to keep a plan up-to-date is to incorporate it within the change management process of the organization. When you think about it, it makes a lot of sense. Where do you document new applications, equipment, or services? Where do you document updates and patches? Your change management process should be updated to incorporate fields and triggers that alert the BCP team when a significant change will occur and should provide a means to update the recovery documentation. What’s the point of removing the dust bunnies off a plan if it has your configurations from three years ago? There is nothing worse than that feeling at the pit of your stomach when you realize the one thing you thought was going to save you will in fact only serve to keep a fire stoked with combustible material.
References

- Disaster Prevention and Recovery Program of the Virginia Community College System  www.so.cc.va.us/its/models/secpl.htm
Life Cycles
Remember that the DRP and BCP have life cycles. Understanding and maintaining each step of the life cycle is critical if these plans are to be useful to the organization.
Chapter 9: Business Continuity and Disaster Recovery

Summary

Although business continuity planning is usually given low priority in most organizations today, that does not mean it is not important and crucial. Unfortunately, many companies have to experience the pain of a disaster to understand how it could have circumvented or mitigated the events that caused the pain to occur.

To develop and carry out business continuity efforts successfully, plenty of thought, planning, time, and effort must go into the different phases of this activity. The real threats must be identified and understood, reasonable countermeasures must be put into place, and detailed plans must be outlined for the unfortunate but anticipated day when they are needed.

Quick Tips

- A business continuity plan (BCP) contains strategy documents that provide detailed procedures that ensure critical business functions are maintained and that help minimize losses of life, operations, and systems.
- A BCP provides procedures for emergency responses, extended backup operations, and post-disaster recovery.
- A BCP should reach enterprise-wide, with individual organizational units each having their own detailed continuity and contingency plans.
- A BCP needs to prioritize critical applications and provide a sequence for efficient recovery.
- A BCP requires senior executive management support for initiating the plan and final approval.
- BCPs can quickly become outdated due to personnel turnover, reorganizations, and undocumented changes.
- Executives may be held liable if proper BCPs are not developed and used.
- Threats can be natural, manmade, or technical.
- The steps of recovery planning include initiating the project, performing business impact analyses, developing a recovery strategy, developing a recovery plan, and implementing, testing, and maintaining the plan.
- The project initiation phase involves getting management support, developing the scope of the plan, and securing funding and resources.
- The business impact analysis is one of the most important first steps in the planning development. Qualitative and quantitative data needs to be gathered, analyzed, interpreted, and presented to management.
- Executive commitment and support are the most critical elements in developing the BCP.
A business case must be presented to gain executive support. This is done by explaining regulatory and legal requirements, exposing vulnerabilities, and providing solutions.

Plans should be prepared by the people who will actually carry them out.

The planning group should comprise representatives from all departments or organizational units.

The BCP team should identify the individuals who will interact with external entities such as the press, shareholders, customers, and civic officials. Response to the disaster should be done quickly and honestly, and should be consistent with any other employee response.

Disaster recovery and continuity planning should be brought into normal business decision-making procedures.

The loss criteria for disasters include much more than direct dollar loss. It may include added operational costs, loss in reputation and public confidence, loss of competitive advantage, violation of regulatory or legal requirements, loss in productivity, delayed income, interest costs, and loss in revenue.

A survey should be developed and given to the most knowledgeable people within the company to obtain the most realistic information pertaining to a company’s risk and recovery procedures.

The plan’s scope can be determined by geographical, organizational, or functional means.

Many things need to be understood pertaining to the working environment so it can be replicated at an alternate site after a disaster.

Subscription services can supply hot, warm, or cold sites.

A reciprocal agreement is one in which a company promises another company it can move in and share space if it experiences a disaster and vice versa. Reciprocal agreements are very tricky to implement and are unenforceable. However, they are cheap and sometimes the only choice.

A hot site is fully configured with hardware, software, and environmental needs. It can usually be up and running in a matter of hours. It is the most expensive option, but some companies cannot be out of business longer than a day without detrimental results.

A warm site does not have computers, but it does have some peripheral devices such as disk drives, controllers, and tape drives. This option is less expensive than a hot site but takes more effort and time to get operational.

A cold site is just a building with power, raised floors, and utilities. No devices are available. This is the cheapest of the three options but can take weeks to get up and operational.

When returning to the original site, the least critical organizational units should go back first.

An important part of the disaster recovery and continuity plan is to communicate its requirements and procedures to all employees.
Chapter 9: Business Continuity and Disaster Recovery

- Testing, drills, and exercises demonstrate the actual ability to recover and can verify the compatibility of backup facilities.
- Before tests are performed, there should be a clear indication of what is being tested, how success will be determined, and how mistakes should be expected and dealt with.
- A checklist test is one in which copies of the plan are handed out to each functional area to ensure the plan properly deals with the area’s needs and vulnerabilities.
- A structured walk-through test is one in which representatives from each functional area or department get together and walk through the plan from beginning to end.
- A simulation test is one in which a practice execution of the plan takes place. A specific scenario is established and the simulation continues up to the point of actual relocation to the alternate site.
- A parallel test is one in which some systems are actually run at the alternate site.
- A full-interruption test is one in which regular operations are stopped and where processing is moved to the alternate site.
- Remote journaling involves transmitting the journal or transaction log offsite to a backup facility.

Questions

Please remember that these questions are formatted and asked in a certain way for a reason. Keep in mind that the CISSP exam is asking questions at a conceptual level. Questions may not always have the perfect answer, and the candidate is advised against always looking for the perfect answer. Instead, the candidate should look for the best answer in the list.

1. What procedures should take place to restore a system and its data files after a system failure?
   A. Restore from storage media backup
   B. Perform a parallel test
   C. Implement recovery procedures
   D. Perform a walk-through test

2. What is one of the first steps in developing a business continuity plan?
   A. Identify backup solution
   B. Decide whether the company needs to perform a walk-through, parallel, or simulation test
   C. Perform a business impact analysis
   D. Develop a business resumption plan
3. How often should a business continuity plan be tested?
   A. At least every ten years
   B. Only when the infrastructure or environment changes
   C. At least every two years
   D. Whenever there are significant changes in the organization

4. During a test recovery procedure, one important step is to maintain records of important events that happen during the procedure. What other step is just as important?
   A. Schedule another test to address issues that took place during that procedure
   B. Make sure someone is prepared to talk to the media with the appropriate responses
   C. Report the events to management
   D. Identify essential business functions

5. Which of the following actions is least important when quantifying risks associated with a potential disaster?
   A. Gathering information from agencies that report the probability of certain natural disasters taking place in that area
   B. Identifying the company’s key functions and business requirements
   C. Identifying critical systems that support the company’s operations
   D. Estimating the potential loss and impact the company would face based on how long the outage lasted

6. The purpose of initiating emergency actions right after a disaster takes place is to prevent loss of life and injuries, and to ______________.
   A. Secure the area to ensure that no looting or fraud takes place
   B. Mitigate further damage
   C. Protect evidence and clues
   D. Investigate the extent of the damages

7. Which of the following is the best way to ensure that the company’s backup tapes can be restored and used at a warm site?
   A. Retrieve the tapes from the offsite facility and verify that the equipment at the original site can read them
   B. Ask the offsite vendor to test them and label the ones that were properly read
   C. Test them on the vendor’s machine, which won’t be used during an emergency
   D. Inventory each tape kept at the vendor’s site twice a month
8. Which best describes a hot-site facility versus a warm- or cold-site facility?
   A. A site that has disk drives, controllers, and tape drives
   B. A site that has all necessary PCs, servers, and telecommunications
   C. A site that has wiring, central air, and raised flooring
   D. A mobile site that can be brought to the company’s parking lot
9. Which is the best description of remote journaling?
   A. Backing up bulk data to an offsite facility
   B. Backing up transaction logs to an offsite facility
   C. Capturing and saving transactions to two mirrored servers in-house
   D. Capturing and saving transactions to different media types
10. Which of the following is something that should be required of an offsite backup facility that stores backed-up media for companies?
    A. The facility should be within 10 to 15 minutes of the original facility to ensure easy access.
    B. The facility should contain all necessary PCs and servers and should have raised flooring.
    C. The facility should be protected by an armed guard.
    D. The facility should protect against unauthorized access and entry.
11. Which item will a business impact analysis not identify?
    A. Whether the company is best suited for a parallel or full-interrupt test
    B. What areas would suffer the greatest operational and financial loss in the event of a particular disaster or disruption
    C. What systems are critical for the company and must be highly protected
    D. What amount of outage time a company can endure before it is permanently crippled
12. Which areas of a company are recovery plans recommended for?
    A. The most important operational and financial areas
    B. The areas that house the critical systems
    C. All areas
    D. The areas that the company cannot survive without
13. Who has the final approval of the business continuity plan?
    A. The planning committee
    B. Each representative of each department
    C. Management
    D. External authority
14. Which are the proper steps for developing a continuity plan?
   A. Project initiation, strategy development, business impact analysis, plan development, implementation, testing, and maintenance
   B. Strategy development, project initiation, business impact analysis, plan development, implementation, testing, and maintenance
   C. Implementation and testing, project initiation, strategy development, business impact analysis, and plan development
   D. Plan development, project initiation, strategy development, business impact analysis, implementation, testing, and maintenance

15. What is the most crucial piece of developing a business continuity plan?
   A. Business impact analysis
   B. Implementation, testing, and following through
   C. Participation from each and every department
   D. Management support

16. During development, testing, and maintenance of the continuity plan, a high degree of interaction and communications is crucial to the process. Why?
   A. This is a regulatory requirement of the process.
   B. The more people who talk about it and are involved, the more awareness will increase.
   C. This is not crucial to the plan and should not be interactive because it will most likely affect operations.
   D. Management will more likely support it.

17. To get proper management support and approval of the plan, a business case must be made. Which of the following is least important to this business case?
   A. Regulatory and legal requirements
   B. Company vulnerabilities to disasters and disruptions
   C. How other companies are dealing with these issues
   D. The impact the company can endure if a disaster hits

18. Which of the following describes a parallel test?
   A. It is performed to ensure that some systems will run at the alternate site.
   B. All departments receive a copy of the disaster recovery plan and walk through it.
   C. Representatives from each department come together and go through the test collectively.
   D. Normal operations are shut down.

19. Which of the following describes a structured walk-through test?
   A. It is performed to ensure that critical systems will run at the alternate site.
B. All departments receive a copy of the disaster recovery plan and walk through it.

C. Representatives from each department come together and go through the test collectively.

D. Normal operations are shut down.

20. When is the emergency actually over for a company?
   A. When all people are safe and accounted for
   B. When all operations and people are moved back into the primary site
   C. When operations are safely moved to the offsite facility
   D. When a civil official declares that all is safe

21. Which of the following does not describe a reciprocal agreement?
   A. The agreement is enforceable.
   B. It is a cheap solution.
   C. It may be able to be implemented right after a disaster.
   D. It could overwhelm a current data processing site.

22. Which of the following describes a cold site?
   A. Fully equipped and operational in a few hours
   B. Partially equipped with data processing equipment
   C. Expensive and fully configured
   D. Provides environmental measures but no equipment

23. Which of the following best describes what a disaster recovery plan should contain?
   A. Hardware, software, people, emergency procedures, recovery procedures
   B. People, hardware, offsite facility
   C. Software, media interaction, people, hardware, management issues
   D. Hardware, emergency procedures, software, identified risk

24. Which of the following is not an advantage of a hot site?
   A. Offers many hardware and software choices
   B. Is readily available
   C. Can be up and running in hours
   D. Annual testing is available

25. Disaster recovery plans can stay updated by doing any of the following except:
   A. Make disaster recovery a part of every business decision
   B. Make sure it is part of employees’ job descriptions
   C. Perform regular drills that use the plan
   D. Make copies of the plan and store them in an offsite facility
Answers

1. C. In this and similar situations, recovery procedures should be followed, which most likely includes recovering data from the backup media. Recovery procedures could include proper steps of rebuilding a system from the beginning, applying the necessary patches and configurations, and ensuring that what needs to take place to ensure productivity is not affected. Some type of redundant system may need to be put into place.

2. C. A business impact analysis includes identifying critical systems and functions of a company and interviewing representatives from each department. Once management’s support is solidified, a business impact analysis needs to be performed to identify the threats the company faces and the potential costs of these threats.

3. D. The plans should be tested if there have been substantial changes to the company or the environment. They should also be tested at least once a year.

4. C. When recovery procedures are carried out, the outcome of those procedures should be reported to the individuals who are responsible for this type of activity, which is usually some level of management. If the procedures worked properly, management should know it, and if problems were encountered, management should definitely be made aware of them. Members of management are the ones who are responsible overall for fixing the recovery system and will be the ones to delegate this work and provide the necessary funding and resources.

5. A. The question asked you about quantifying the risks, which means to calculate the potential business impact of specific disasters. The core components of a business impact analysis are
   - Identifying the company’s key functions and business requirements
   - Identifying critical systems that support the company’s operations
   - Estimating the potential loss and impact the company would face based on how long the outage lasted

Gathering information from agencies that report the probability of certain natural disasters taking place in that area is an important piece in determining the probability of these threats, but it is considered least necessary when quantifying the potential damage that could be experienced.

6. B. The main goal of disaster recovery and business continuity plans is to mitigate all risks that could be experienced by a company. Emergency procedures first need to be carried out to protect human life and then other procedures need to be executed to reduce the damage from further threats.

7. A. A warm site is a facility that will not be fully equipped with the company’s main systems. The goal of using a warm site is that, if a disaster takes place, the company will bring its systems with it to the warm site. If the company cannot bring the systems with it because they are damaged, the company
must purchase new systems that are exactly like the original systems. So, to properly test backups, the company needs to test them by recovering the data on its original systems at its main site.

8. B. A hot site is a facility that is fully equipped and properly configured so that it can be up and running within hours to get a company back into production. Answer B gives the best definition of a fully functionally environment.

9. B. Remote journaling is a technology used to transmit data to an offsite facility, but this usually only includes moving the journal or transaction logs to the offsite facility, not the actual files.

10. D. This question addresses a facility that is used to store backed-up data; it is not talking about an offsite facility used for disaster recovery purposes. The facility should not be only 10–15 minutes away because some types of disaster could destroy both the company’s main facility and this facility if they are that close together, in which case the company would lose all of its information. The facility should have the same security standards as the company’s security, including protection against unauthorized access.

11. A. All the other answers address the main components of a business impact analysis. Determining the best type of exercise or drill to carry out is not covered under this type of analysis.

12. C. It is best if every department within the company has its own contingency plan and procedures in place. These individual plans would “roll up” into the overall BCP enterprise plan.

13. C. Management really has the final approval over everything within a company, including these plans.

14. A. These steps outline the processes that should take place from beginning to end pertaining to these types of plans.

15. D. Management’s support is the first thing to obtain before putting any real effort into developing these plans. Without management’s support, the effort will not receive the necessary attention, resources, funds, or enforcement.

16. B. Communication not only spreads awareness of these plans and their contents, but also allows more people to discuss the possible threats and solutions, which may lead to ideas that the original team did not consider.

17. C. The other three answers are key components when building a business case. Although it is a good idea to investigate and learn about how other companies are dealing with similar issues, it is the least important of the four items listed.

18. A. In a parallel test, some systems are run at the alternate site and the results are compared with how processing takes place at the primary site. This is to ensure that the systems work in that area and productivity is not affected. This also extends the previous test and allows the team to walk through the steps of setting up and configuring systems at the offsite facility.
19. C. During a structured walk-through test, functional representatives review the plan to ensure its accuracy and that it correctly and accurately reflects the company's recovery strategy.

20. B. The emergency is not actually over until the company moves back into its primary site. The company is still vulnerable and at risk while it is operating in an altered or crippled state. This state of vulnerability is not over until the company is operating in the way it was prior to the disaster. Of course, this may mean that the primary site has to be totally rebuilt if it was destroyed.

21. A. A reciprocal agreement is not enforceable, meaning that the company that agreed to let the damaged company work out of its facility can decide not to allow this to take place. A reciprocal agreement is a better secondary backup option if the original plan falls through.

22. D. A cold site only provides environmental measures—wiring, air conditioning, raised floors—basically a shell of a building and no more.

23. A. The recovery plan should contain information about how to deal with people, hardware, software, emergency procedures, recovery procedures, facility issues, and supplies.

24. A. Because hot sites are fully equipped, they do not allow for a lot of different hardware and software choices. The subscription service offers basic software and hardware products and does not usually offer a wide range of proprietary items.

25. D. The plan should be part of normal business activities. A lot of time and resources go into creating disaster recovery plans, after which they are usually stored away and forgotten about. They need to be updated continuously as the environment changes to ensure that the company can properly react to any type of disaster or disruption.