One thing to keep in mind for DR/BC plans is that disasters aren't always limited to the organization. A disaster in a geographic region may mean that both the organization and its employees will be affected by it. Employees must personally respond to the same disaster. If employees must respond to the disaster at home with their own families, they may not be in a position to help the organization respond to the disaster as well.

### DR/BC Plan Development

Many of the steps in the DR/BC planning process are similar to the RA and IR planning processes. Contingency planning is a part of risk management. The steps in the DR/BC planning process are:

- Develop the DR/BC policy
- Conduct a business impact analysis
- Identify threats and potential controls
- Determine recovery strategy
- Design and maintain the plan

The DR/BC team must make sure that policies and plans are in place that help the organization complete these steps. The DR/BC policy is a statement of executive management's commitment to the business continuity planning. It should state the purpose and goals of DR/BC. The policy should define DR/BC roles and responsibilities. The policy should include the organization's resource requirements for any DR/BC plan.

After a DR/BC policy is approved, the DR/BC team must conduct a **business impact analysis (BIA)**. A BIA identifies key business operations. It also identifies the resources that support those operations. The DR/BC team uses a BIA to estimate how long those critical operations and resources can be offline before the organization's entire business is negatively affected.

To complete a BIA, the DR/BC team must:

- **Identify critical business processes**—The BR/DR team must identify the organization's critical business processes. There's no master list of processes that are critical to all organizations. Each organization is different. Some critical processes might include payroll, attendance scheduling, and customer service activities.
- **Identify IT resources that support critical business processes**—The BR/DR team must identify the resources that support its critical business processes. Resources can include the organization's communications infrastructure. They also can include individual IT systems and components.
- **Determine how long IT resources can be offline**—The DR/BC team must identify the effect on business organizations if a resource is disrupted or damaged and a critical process can't run.
- **Determine recovery criticality**—The DR/BC team must prioritize how the organization will handle IT resources and business processes following a disaster.

A BIA closely resembles a risk assessment. Many of the same tools and techniques used in an RA are used to complete a BIA. The team can interview employees throughout the organization to learn about its many business processes. The team also could send a questionnaire to a sampling of employees. The questionnaire could ask questions about business processes and resources.

Once the DR/BC team determines the organization's critical processes and resources, it must figure out how long those processes and resources can be offline before the organization experiences irreparable harm. This period is called **maximum tolerable downtime (MTD)**. Some processes and systems are so critical that they can be down only for a few minutes before an organization suffers irreparable damage. If these processes are offline longer than the MTD, the organization might fail. Processes and systems that aren't essential to business operations may have an MTD of days or weeks.

> **NOTE**
>
> Some resources use the term *maximum acceptable outage (MAO)* in place of MTD. The two terms mean the same thing.

The DR/BC team must determine the order in which IT resources will be handled and restored following the disaster. It uses the results of the BIA to make this determination. If an organization must resume a business process within a short period, it will need to make sure that it can put people and processes in place to recover the process within that period. The priority list of processes and resources helps executive management make recover strategy decisions.

After the BIA is complete, the DR/BC team must identify threats and potential controls. This step is very similar to a risk assessment. In fact, the organization may have completed this exercise as part of an RA. If so, the DR/BC team can use those results at this step.

The DR/BC team must identify the threats to the organization that have disaster potential. It also must identify potential controls to respond to those threats. These controls try to reduce the possibility of the organization experiencing a disaster. If a disaster can't be avoided, these controls may lessen the amount of damage to the organization.

For example, an organization's data center may be located in an area prone to tornadoes. If the organization can't move its data center, it may try to fortify it. The organization might try to make the data center more resistant to wind-related damage to protect its business processes.

Some common preventative controls that an organization can implement include:

- Fire detection and suppression systems
- Installing backup generators or uninterruptible power supplies
- Offsite storage of system backup media
- Frequent backups of critical data
- Extra equipment inventories for critical IT resources

The DR/BC team also must determine a recovery strategy. It consults with executive management to do this. An organization's recovery strategy addresses the resources that it must recover after a disaster. An organization will have to consider a wide variety of recovery strategies.

An organization must prepare recovery strategies for its:

- **Critical business processes**—The organization must plan for recovering its business processes. It must understand all the workflow steps needed to complete a business process. It must know the resources and supplies needed to support these processes.
- **Facilities and supplies**—The organization must make sure that it has a plan to restore its main facility. It also must restore the utilities needed to support that facility. Utilities include telecommunications and electrical infrastructure.

### Backup Site Options

It's rare when an organization experiences a disaster that forces it out of its main facility for a long time. However, the organization still must plan for this possibility. It must have a location to which it can move its operations. This is called a *backup site*. An organization has several planning options for a backup site. It's important for you to know the differences between them.

A **mirrored site** is a fully operational backup site. It actively runs the organization's IT processes in parallel with the organization's main facility. A mirrored site is a redundant facility. An organization can immediately transfer all of its IT operations to the mirrored site. This site is already staffed with the organization's employees. This is the most expensive type of backup site to maintain. This type of backup site is appropriate for organizations that have a low MTD for critical processes. This type of backup site supports high availability.

A **hot site** is an operational backup site. It has all of the equipment and infrastructure that an organization needs to continue its business operations. The equipment in the hot site is fully compatible with the organization's main facility. A hot site can become operational within minutes to hours after a disaster. It's not staffed with people. It also doesn't process data in parallel with the main facility. The organization will need to bring data backups to the hot site facility. A hot site is expensive to maintain. It may be the best choice for an organization that can afford some, but not a lot, of downtime.

A **warm site** is a compromise between a hot site and a cold site. A warm site is space that contains some, but not all, of the equipment that an organization will need to continue operations in the event of a disaster. The warm site is partially prepared for operations. It has electricity and network connectivity. This type of site is more expensive than a cold site.

A **cold site** is a backup site that's little more than reserved space. It's the most inexpensive type of backup site. It doesn't have any equipment or hardware set up. It will have electrical service. It most likely won't have network connectivity. It can take weeks for an organization to get a cold site ready for business operations. An organization will have to acquire equipment and infrastructure to make the site operational.

- **Employee environment**—The organization must have plans in place for supporting its employees during a disaster. This means making sure that it has ways to communicate with employees during a disaster. The organization also must have plans in place to manage employee responsibilities until the organization can return to normal operations.
- **IT operations**—The organization must have plans in place to resume its IT operations. This means making sure that infrastructure components are in place so that business can resume. The organization will want to have contracts with its vendors so that it can get replacement equipment quickly.
- **Data recovery**—The organization must have a way to recover its data and operational information. It must have plans in place to retrieve data from offsite storage facilities. It also must have plans to retrieve paper-based information from its main facility.

A recovery strategy also must include the people that will implement it. A team with specialized skills and knowledge must head each recovery area. For example, the organization's storage administrators should serve on the team in charge of data recovery. Each team must have a leader.

Once an organization develops its DR/BC plan, it must monitor and update it in response to changing conditions. An organization must update its plan anytime its business processes or technology change. It must update the plan any time key personnel change. Organizations put contingency plans in place so that they can respond to events that adversely affect them. It's not enough to create a plan and put it away on a shelf for use "just in case."

A DR/BC plan helps an organization respond to a disaster. These plans are an important part of an organization's risk management activities. The DR/BC planning process is shown in Figure 14-3.

## Testing the Plan

Organizations must test their contingency plans on a regular basis to make sure that the plan accounts for all critical business functions and processes. It also should test its contingency plans to make sure that the plans don't have any deficiencies. An organization must correct plan deficiencies.

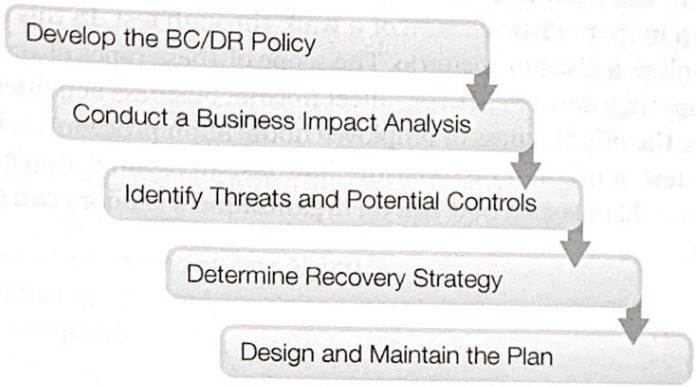


**FIGURE 14-3** DR/BC planning process.

Contingency plan testing has a number of objectives. They include:

- Help employees become familiar with and accept the DR/BC plan.
- Train employees how to respond during an emergency.
- Identify weaknesses or deficiencies within the plan.
- Make sure that all of the checklists and procedures needed to implement the plan are created and in place.
- Make sure that all the resources and supplies needed to implement the plan are in place and are operational.
- Make sure that all communications mechanisms work properly.
- Make sure that all DR/BC teams are able to work well together.

> **NOTE**
>
> In the DR/BC plan context, a single point of failure is a step in the plan or an assumption within the plan that is critical to the performance of the entire plan. If that step or the assumption fails, then a critical portion of the plan, or the entire plan, could fail.

Through testing, an organization can learn that it's missing key business process areas. It also can identify single points of failure within the plan and take steps to correct them. Any changes that are made to the DR/BC plan as part of the test review must be fully documented. Changes to the plan also must be communicated to all members of the organization.

There are five ways to test DR/BC plans. These tests also could be used to test an organization's incident response capability.

A **checklist test** is one of the most basic types of DR/BC test. In this type of test, the DR/BC team makes sure that supplies and inventory items that are needed to execute the DR/BC plan are in place. This type of test makes sure that sufficient supplies are stored at backup facilities. It also makes sure that the organization has enough resource copies of the DR/BC plan and that all copies have current information.

A **walk-through test** is often used with a checklist test. In this type of test, the DR/BC team "walks through" the entire DR/BC plan. They study each area of the plan to make sure that all of the assumptions and tasks listed in it are correct. This type of test also helps the people who are responsible for executing the DR/BC plan become very familiar with it. This type of test is sometimes called a tabletop walk-through test or tabletop test because members of the team will sit around a table as they study the plan.

A **simulation test** is a more realistic version of a walk-through test. In this type of test, the organization role-plays a disaster scenario. The steps of these types of tests have to be carefully defined so that they don't negatively affect normal business activities. This test is designed to measure the effectiveness of employee notification procedures. Depending upon the scope of the test, it might try to measure how fast an organization can set up its backup site. It also could measure how fast an organization's vendors can provide additional equipment.

Contingency plan testing has a number of objectives. They include:

- Help employees become familiar with and accept the DR/BC plan.
- Train employees how to respond during an emergency.
- Identify weaknesses or deficiencies within the plan.
- Make sure that all of the checklists and procedures needed to implement the plan are created and in place.
- Make sure that all the resources and supplies needed to implement the plan are in place and are operational.
- Make sure that all communications mechanisms work properly.
- Make sure that all DR/BC teams are able to work well together.

> **NOTE**
> In the DR/BC plan context, a single point of failure is a step in the plan or an assumption within the plan that is critical to the performance of the entire plan. If that step or the assumption fails, then a critical portion of the plan, or the entire plan, could fail.

Through testing, an organization can learn that it's missing key business process areas. It also can identify single points of failure within the plan and take steps to correct them. Any changes that are made to the DR/BC plan as part of the test review must be fully documented. Changes to the plan also must be communicated to all members of the organization.

There are five ways to test DR/BC plans. These tests also could be used to test an organization's incident response capability.

A **checklist test** is one of the most basic types of DR/BC test. In this type of test, the DR/BC team makes sure that supplies and inventory items that are needed to execute the DR/BC plan are in place. This type of test makes sure that sufficient supplies are stored at backup facilities. It also makes sure that the organization has enough reference copies of the DR/BC plan and that all copies have current information.

A **walk-through test** is often used with a checklist test. In this type of test, the DR/BC team "walks through" the entire DR/BC plan. They study each area of the plan to make sure that all of the assumptions and tasks stated in it are correct. This type of test also helps the people who are responsible for executing the DR/BC plan become very familiar with it. This type of test is sometimes called a *tabletop walk-through test* or *tabletop test* because the members of the team will sit around a table as they study the plan.

A **simulation test** is a more realistic version of a walk-through test. In this type of test, the organization role-plays a disaster scenario. The scope of these types of tests has to be carefully defined so that they don't negatively affect normal business activities. This test is designed to measure the effectiveness of employee notification procedures. Depending upon the scope of the test, it might try to measure how fast an organization can set up its backup site. It also could measure how fast an organization's vendors can provide additional equipment.

**FYI**

Organizations with critical business functions that affect many customers tend to be serious about DR/BC planning and testing. AT&T has a Network Disaster Recovery Team. The team is responsible for restoring voice and data network communications to an area that's affected by a disaster. The team conducts four disaster recovery exercises each year. It was deployed in 2013 to respond to wildfires in Colorado and California. You can read about the team's efforts at *http://www.corp.att.com/ndr/*.

A **parallel test** is designed to test the organization's IT recovery processes. In this type of test, the organization tests its ability to recover its IT systems and its business data. The organization brings its backup sites online. It will then use historical business data to test how those systems operate. In this test, the organization tests both data processing and data recovery. During the test, the organization continues normal business operations at its main facility. The test is conducted using historical data.

A **full interruption test** is designed to test the organization's entire DR/BC plan. This test involves a scenario that destroys or severely damages the organization's main facility. The organization must transfer all business and IT functions to its backup site. In this type of test, all normal business operations stop. Operations are shut down at the main site. They must be transferred to the backup site using the processes stated in the DR/BC plan.

A full interruption test is the most expensive kind of contingency plan test. It can help the organization learn a lot about its DR/BC plan's effectiveness. However, it also has the potential to negatively affect the organization's business. If the organization can't get business operations resumed at the backup site, then the test itself can create a disaster situation for the organization. Organizations undertake these types of tests with great care.

## Special Considerations

Risk management and contingency planning activities make good business sense. They help an organization prepare for threats and events that harm its ability to meet its business goals. Organizations that engage in these activities understand their information security posture. They know where they have weaknesses. They know the threats to the confidentiality, integrity, and availability of their IT resources and data.

### Addressing Compliance Requirements

For many organizations, RM and contingency planning aren't just good business practices. Sometimes they are required by law. Many laws require the organizations they cover to complete risk assessments and create contingency plans. Table 14-5 reviews some laws that have these requirements.

**TABLE 14-5** Laws with risk assessment and contingency plan requirements.

| NAME OF LAW | RISK ASSESSMENT REQUIRED? | DR/BC PLAN REQUIRED? |
|---|---|---|
| Gramm-Leach-Bliley Act<br>Consumer financial information | Yes | Yes |
| Payment Card Industry Standards*<br>Companies that accept credit cards for payment | Yes | Yes |
| Health Insurance Portability and Accountability Act<br>Protected health information | Yes | Yes |
| Sarbanes-Oxley Act<br>Corporate financial information | Yes | Implied if contingency plans are indicated as an internal control required to secure financial reporting processes and systems. |
| Federal Information Systems Management Act<br>Federal information systems | Yes | Yes |

*The Payment Card Industry (PCI) Standards are not a law. Organizations that wish to accept credit cards for payment of goods and services must follow these standards. Banks that process credit card information enforce PCI compliance.

## When to Call the Police

Children learn the basics of "when to call 9-1-1" at a very early age. Children are taught to call the police or emergency responders when:

- Someone's life is in immediate danger
- When smoke or fire is present
- When emergency medical help is needed
- When a crime is being committed

These are good rules for an organization as well. Organizations should include rules for when to call law enforcement or emergency responders in their contingency plans.

### Must People Report Crime?

Under common law, in general, a person has no duty to report a crime that he or she witnesses. For purposes of the law, an organization is considered a "person." Thus, most organizations also have no obligation to report crimes they witness.

There are some instances where people are required by law to report crimes, however. For instance, most people are required to report crimes where children or vulnerable adults are in danger. These laws require people to report suspected child abuse and neglect to law enforcement.

Some states have laws that require information technology workers to report the discovery of child pornography on computers. They must report the discovery to law enforcement. The IT worker must have discovered the pornography within the scope of his or her employment. An IT worker isn't required to search for this type of material. However, if it is discovered, he or she must report it. At the time that this was written, 10 states had such laws.[9]

Most organizations should report any criminal activity that involves their IT resources or data. It's important to contact law enforcement right away to start investigating the crime.

Sometimes it's hard to know if a crime is committed. If the organization experiences a data breach, it's likely that a crime upon the organization was committed. Possible crimes include trespass, theft of data, theft of resources, unauthorized access, and similar crimes.

One of the most important reasons to promptly report crimes involving IT resources is so that forensic evidence can be collected. This type of evidence can be used to investigate computer crimes. However, this type of evidence is very volatile and must be preserved properly.

One of the things that organizations must account for in their contingency plans is the fact that communications systems will likely be overloaded in a regional disaster or emergency. It may take time to contact first responders. It may take extra time to receive their assistance. In regional natural disaster situations, people are usually discouraged from calling emergency responders unless a person's life is in immediate danger. This is to keep emergency phone lines, such as 9-1-1 trunk telephone lines, from being overloaded with calls.

## Public Relations

An organization's contingency plans must consider its public relations strategy. **Public relations (PR)** is a marketing field that manages an organization's public image. It includes marketing the organization's products and services. It protects the organization's reputation and image. PR includes responding to crises that threaten that image.

An organization's PR team develops communication strategies. These strategies are used to guide communications with employees, customers, and stakeholders. Coordinating an organization's public message is sometimes difficult under normal business operations. It's more difficult in an emergency. A PR strategy for emergencies must consider:

- Who is authorized to make comments on the organization's behalf?
- Who is authorized to approve the contents of comments shared with the public?
- How often should information be shared with the public?
- How should information be shared with the public?
- How should information be shared if normal communications methods are unavailable in an emergency?

It's important that an organization have a PR strategy for emergencies. The organization must make sure that information is given to stakeholders in a reliable and organized manner. It also must make sure that reliable information is communicated to employees. An organization's reputation can suffer if it doesn't share enough information or shares it in a chaotic manner. Its reputation also can be harmed if the organization distributes conflicting information from different sources.

## CHAPTER SUMMARY

This chapter reviewed risk management and contingency planning concepts. The RM process helps an organization understand the risks that it faces each day. It also helps organizations strengthen their security posture in response to threats and vulnerabilities. Many laws require organizations to use RM concepts to create information security programs.

This chapter also reviewed different types of contingency plans. An organization uses contingency plans to limit financial loss due to an adverse event. Contingency plans help minimize the length of time that an organization's services and critical processes are interrupted after an emergency.