Chapter 4

Business Impact Analysis

Solutions in this chapter:

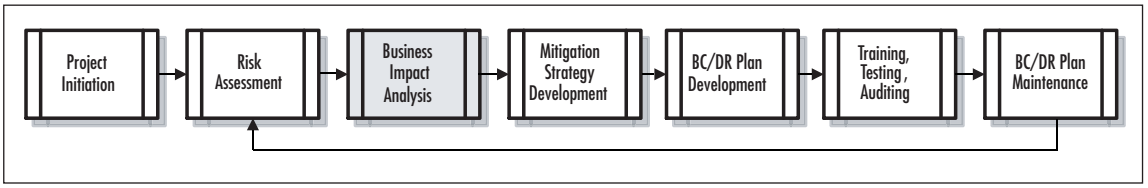
- **Business Impact Analysis Overview**
- **Understanding Impact Criticality**
- **Identifying Business Functions and Processes**
- **Gathering Data for the Business Impact Analysis**
- **Determining the Impact**
- **Business Impact Analysis Data Points**
- **Preparing the Business Impact Analysis Report**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

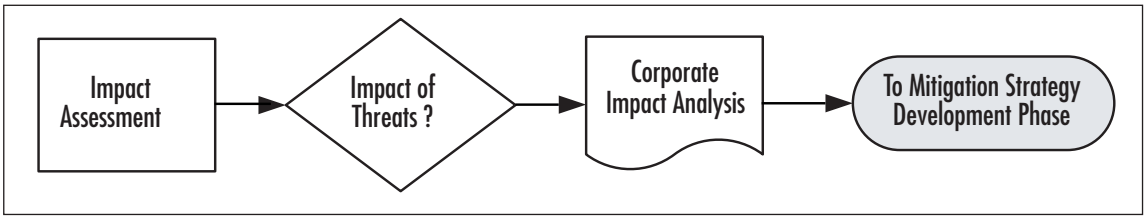
In Chapter 3, you learned about risk management and the process for assessing risks. In this chapter, we turn our attention to the process of business impact analysis. Risk assessment looks at the various threats your company faces; business impact analysis looks at the critical business functions and the impact of not having those functions available to the firm. These two assessments look at the company from two different angles. The risk assessment starts from the threat side, and the business impact analysis starts from the business process side. When you're managing general business risk, you might actually start with the business impact analysis. However, in planning for business continuity as an outgrowth of disaster recovery, it makes more sense to understand the full picture regarding risks and threats and then look at business impact. However, if you have a methodology you use that starts with business impact analysis, that's fine. Both outputs—from the risk assessment and the business impact analysis phases—are used as input to the mitigation strategy development. As long as you have those ready before you start the mitigation phase, which we'll discuss in Chapter 5, you should be all set. Figure 4.1 depicts where we are in the planning process thus far.

Figure 4.1 Business Continuity and Disaster Recovery Planning Process



You can see, in Figure 4.2, that we'll be focusing on the third and final segment of the risk assessment phase introduced in Chapter 3 (refer to Figure 3.2 in Chapter 3 for the full diagram). In this chapter, we're going to concentrate on the impact of various business functions on your operations. We'll begin with discussing the general framework of performing a business impact analysis and conclude with the specifics of performing an impact analysis for your business continuity and disaster recovery (BC/DR) plan.

Figure 4.2 Impact Assessment Process



Business Impact Analysis Overview

The fundamental task in business impact analysis (BIA) is understanding which processes in your business are vital to your ongoing operations and to understand the impact the disruption of these processes would have on your business. From an IT perspective, as the National Institute of Standards and Technology (NIST) views it: "The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components." (*Source*: NIST "Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34, p. 16). So, there are two parts to the BIA: the first is to understand mission-critical business processes and the second is to correlate those to IT systems.

As an IT professional, you certainly understand the importance of various IT systems, but you may not be fully aware of the critical business functions performed in your company. Even if your role in this project is limited to managing the IT elements in this BC/DR plan, you should still pay close attention to the material in this chapter for two main reasons. First, understanding the critical business functions is important in terms of understanding how to recover IT systems in the event of a significant business disruption. You might think that System A is most critical, based on a number of assumptions you're making. However, through this process, you might find that System B or C is really what keeps the company up and running on a day-to-day basis or that without System D, System A doesn't really matter. Second, if you have any aspirations at all of moving up the corporate ladder toward that CIO job, your understanding of the overall business will certainly help you achieve those goals. Today's CIO needs to have a solid background in technology *and* business, so understanding the critical business functions in your company will pay off in many ways for you.

According to the Business Continuity Institute (www.thebci.org), a recognized leader in business continuity management and certification, there are four primary purposes of the business impact analysis:

- Obtain an understanding of the organization's most critical objectives, the priority of each, and the timeframe for resumption of these following an unscheduled interruption.
- Inform a management decision on Maximum Tolerable Outage (MTO) for each function.
- Provide the resource information from which an appropriate recovery strategy can be determined/recommended.
- Outline dependencies that exist both internally and externally to achieve critical objectives.

Source: The Business Continuity Institute, Good Practices Guidelines, 2005, p. 21.

Business impact analysis is the process of figuring out which processes are critical to the company's ongoing success, and understanding the impact of a disruption to those processes. Various criteria are used including customer service, internal operations, legal or regulatory, and financial. From an IT perspective, the goal is to understand the critical business functions and tie those to the various IT systems. As part of this assessment, the interdependencies need to be fully understood. Understanding these interdependencies is critical to both disaster recovery and business continuity, especially from an IT perspective. Would it make sense for your IT staff to spend three days trying to recover System D if System A is still out of commission? Until you perform the BIA, there may be no real way to know.

Business impact analysis includes the steps listed earlier, but we can break them out into a few more discrete activities or steps:

1. Identify key business processes and functions.
2. Establish requirements for business recovery.
3. Determine resource interdependencies.
4. Determine impact on operations.
5. Develop priorities and classification of business processes and functions.
6. Develop recovery time requirements.
7. Determine financial, operational, and legal impact of disruption.

The result of performing these seven steps is a formal business impact analysis, which is used in conjunction with the risk assessment analysis to develop mitigation strategies (discussed in Chapter 5).

The two primary impact points of any business disruption are the operational impact and the financial impact. The operational impact addresses the nonmonetary impact including how people, processes, and technology are impacted by a business disruption and how best to address that impact. The financial impact addresses the monetary impacts and how a business disruption will impact the company's revenues.

Upstream and Downstream Losses

In addition to the direct impact of a business disruption such as an earthquake or flood, there are also indirect impacts you should consider. These can be viewed as upstream and downstream losses. *Upstream losses* are those you will suffer if one of your key suppliers is affected by a disaster. If your company relies on regular deliveries of products or services by another company, you could experience upstream losses if that company cannot deliver. If you run a manufacturing company that relies on raw materials arriving on a set or regular schedule, any disruption to that schedule will impact your company's ability to make and sell its products. This is how a disaster elsewhere can impact you, even if your company is unharmed. *Downstream losses* occur when key customers or the lives in your community are

affected. If your business supplies parts to a major manufacturer that is shut down due to a hurricane or earthquake, your sales will certainly suffer. Similarly, if your company provides any type of noncritical service to your community and there is a flood or landslide, your sales could take a hit while residents of the community deal with the disaster. If you operate a chain of restaurants or movie theaters or golf courses, residents will be more focused on dealing with the disaster than on entertainment and leisure pursuits. These are considered downstream losses even if your business, itself, has not taken the direct impact of a disaster.

Keep in mind, too, that people, businesses, and communities are interrelated; very few (if any) companies exist in isolation. A natural disaster or serious disruption can create a chain reaction that ripples through the business community and impacts the local or regional economy.

From the Trenches…

Protecting Your Assets

Business continuity and disaster recovery planning can certainly help you mitigate some of your risks. In Chapter 5, we'll develop specific strategies for doing so. However, keep in mind that various types of insurance can help as well. This is considered *risk transference* and is a well-accepted business practice. Consider looking into business income interruption and extra expense insurance. If a business disruption occurs, you could have both an immediate and long-term impact to your company's revenues. Not only will it not be business-as-usual, you'll have the added expenses of lost productivity, lost customers, and higher costs. Some of your out-of-pocket expenses might ultimately be covered by insurance, such as the loss of equipment from a storm or building collapse. Other expenses, however, won't be covered. When revenues decrease and expenses increase, it can create a devastating financial picture for your company. Some basic business insurance policies cover expenses and loss of net business income, but it may not cover business interruptions that occur away from your business, such as to your key supplier, vendor, customer, or even your utility company. This type of insurance can typically be purchased as additional coverage to an existing policy. We're not suggesting you purchase additional insurance (and we have no connections to the insurance industry), but we do suggest you look at your financial exposure and your current insurance policy and decide if you're properly protected. Of course, insurance alone will not protect your business from failing in the face of a serious disruption or event—that's where a solid BC/DR plan comes in.

Understanding the Human Impact

Although this chapter is focused on recovering business systems, it's clear that people are a major factor in business continuity efforts—not only from a planning and implementation perspective but from the impact perspective as well. If a natural disaster strikes, it's possible that some or all of your company's employees will be impacted. It's possible that some may die or be seriously injured. Although no one likes to think about these possibilities, they cannot be ignored in a BC/DR plan. As you assess business functions and business processes, you'll also need to identify key positions, key knowledge, and key skills needed for business continuity. In some sense, this begins to cross over into what is traditionally called *succession planning*. In publicly traded companies or high profile start ups, the company often purchases what's called *key man insurance*. This insurance covers the cost of losing a high ranking executive in the company, the assumption being that if someone at that level were suddenly unavailable to carry out that function, the business would suffer financial losses.

Key Positions

Succession planning in companies covers many areas, but typically it's discussed in terms of replacing key employees as well as how to transfer the reins of the company from one leader to the next. Succession planning can include training employees to move up the corporate ladder and assume leadership positions. From a risk management perspective, it can also address who will replace key employees in the event of a planned or unplanned departure. For example, if a company was started by a couple of business partners, at some point before their retirement, they should spend time identifying their successors—whether family members or trusted employees—and identifying the path to hand over the leadership of the company. When done in a thoughtful and predetermined manner, this can help smooth the transition. In terms of BC/DR, this plan can help identify who should step up should something happen to the company's founders or executives.

Beyond key man succession and planning, the BC/DR plan needs to look at key positions within the company and understand the role of each in the business continuity realm. For example, if you have complex database applications, you may identify a database administrator (DBA) as a key role in the business recovery process. Ideally, your existing database administrator would take care of this, but what if she was unable to respond to the business disruption because she was injured or unable to get to the site (or worse)? Rather than identifying specific people, you should identify roles, responsibilities, skills, and knowledge needed. Even though you'd prefer your own DBA to recover the system, if she was unavailable for any reason, you would know that you need a DBA to recover your systems and you could go to external sources to locate a temporary or permanent DBA replacement.

Human Needs

Beyond replacing needed skills and positions, it's important to keep the human impact in mind throughout your planning. As mentioned earlier in the book, everyone responds to disasters differently. If a portion of the building catches on fire and burns, it's likely that those employees in the area at the time the fire breaks out will experience the event in a variety of ways. Some people will evacuate and stand in the parking lot laughing about the close call, even as the fire engines pull in. Others probably will be frightened by the experience and may become shaky, disoriented, or panicky. Still others might seem fine immediately afterward but days or weeks later, they begin to display odd behavior that might be the result of a delayed onset of stress from the event. Clearly, the bigger the event (earthquake, tornado, hurricane), the bigger the human toll in terms of death, injury, and emotional distress.

A good business continuity plan will address the human factors for two reasons. First, addressing employee needs is simply the right thing to do. Although there are companies that may demand that employees report to work following a serious business disruption or face termination, most companies understand that everyone will have different needs. Some may report back to work, some may need to deal with family problems, some may be physically or emotionally unable to return to work immediately. The company's policies with regard to employee needs and requirements in the aftermath of a business disruption or natural disaster should be developed by your Human Resources department; however your BC/DR plan must take these varied responses into consideration. If your IT systems recovery effort hinges on two experienced network administrators, you need to address these as risks in your plan and develop mitigation strategies along with them.

The second reason for addressing employee needs in your BC/DR plan is because it makes good business sense. The ideal scenario might be that everyone is fine and shows up to work, but reality is often far different from that. You can demand that people show up all you want, but if faced with a choice between work and family, between work and health, people will usually choose family and health first. In some cases, insisting people return to work before they are ready can make things worse—they may not be able to concentrate and therefore may make recovery efforts worse instead of better. Incorporating this reality into your plan will mean that you and your team come up with appropriate alternatives that can address the lack of key staff in the aftermath of a business disruption. This helps the employees who may be unable to come back immediately and also helps the company recover in the fastest, most efficient manner possible.

We won't dwell on the human element in this chapter, but we will mention it again in key places to keep it foremost in your mind so that as you determine the impact of various risks, you can also keep the human factor in mind.

Understanding Impact Criticality

As you're thinking about your company and its critical functions, which we'll review following this section, you should keep a rating scale in mind. Later, after you've compiled your list, you can assign a "criticality rating" to each business function. It's important to have an idea of your rating system in mind before you review your business functions so you can spend the appropriate amount of time and energy on mission-critical functions and less time on minor functions. For example, when you sit down with the finance group, you want to keep them focused on defining the mission-critical business functions while listing all business functions that would be needed for business continuation.

Criticality Categories

You can develop any category system that works for you but as with all rating systems, be sure the categories are clearly defined and that there is a shared understanding of the proper use and scope of each. Here is one commonly used rating system for assessing criticality:

- Category 1: Critical Functions–Mission-Critical
- Category 2: Essential Functions–Vital
- Category 3: Necessary Functions–Important
- Category 4: Desirable Functions–Minor

Obviously, your business continuity plan will focus the most time and resources on analyzing the critical functions first, essential functions second. It's possible you will delay dealing with necessary and desirable functions until later stages of your business recovery. Many companies identify these four areas and set timelines for when each of these categories will be functional following a business disruption. Let's look at each category in more detail. You can use these category descriptions as-is or you can tweak them to meet your company's unique needs.

Mission-Critical

Mission-critical business processes and functions are those that have the greatest impact on your company's operations and potential for recovery. Almost everyone working in a company has an innate understanding of the mission-critical operations within their department. The key is to gather all that data and develop a comprehensive look at your mission-critical processes and functions from an organizational perspective. What are the processes that must be present for your company to do business? These are the mission-critical functions. One way to get people to focus on the mission-critical functions is to ask (whether through questionnaire, interview, or workshops) what the first three to five things people would do in their department following a business disruption once the emergency or imminent threat

of a business disruption subsides. This often gives you the clearest view of the mission-critical business functions in each department.

From an IT perspective, the network, system, or application outage that is mission-critical would cause extreme disruption to the business. Such an outage often has serious legal and financial ramifications. This type of outage may threaten the health, well-being, and safety of individuals (hospital systems come to mind). These systems may require significant efforts to restore and these efforts are almost always disruptive to the rest of the business (in the case that any other parts of the business are actually able to function during such an outage). The tolerance for such an outage, whether from the IT system or the function/process it provides, is very low and the recovery time requirement is often described in terms of hours, not days.

Vital

Some business functions may fall somewhere between mission-critical and important, so you may choose to use a middle category that we've labeled "vital" or "essential." How can you distinguish between mission-critical and vital? If you can't, you may not need to use this category. However, you might decide that certain functions are absolutely mission-critical and others are extremely important but should be addressed immediately after the mission-critical functions. Vital functions might include things like payroll, which on the face of it might not be mission-critical in terms of being able to get the business back up and running immediately but which can be vital to the company's ability to function beyond the disaster recovery stage.

From an IT perspective, vital systems might include those that interface with mission-critical systems. Again, this distinction may not be helpful for you. If not, don't try to force your systems into this framework; simply don't use this category. You'll end up with just three categories—mission-critical, important, and minor. If that works for you, that's fine. If you use this category, your recovery time requirement might be measured in terms of hours or a day or two.

Important

Important business functions and processes won't stop the business from operating in the near-term but they usually have a longer-term impact if they're missing or disabled. When missing, these kinds of functions and processes cause some disruption to the business. They may have some legal or financial ramifications and they may also be related to access across functional units and across business systems.

From an IT perspective, these systems may include e-mail, Internet access, databases, and other business tools that are used in a support function, whether to support business functions or IT functions. If disabled, these systems take a moderate amount of time and effort

(as compared to mission-critical) to restore to a fully functioning state. The recovery time requirement for important business processes often is measured in days or weeks.

Minor

Minor business processes are often those that have been developed over time to deal with small, recurring issues or functions. They will not be missed in the near-term and certainly not while business operations are being recovered. They will need to be recovered over the longer-term. Some minor business processes may be lost after a significant disruption and in some cases, that's just fine. Many companies develop numerous processes that should at some point be reviewed, revised, and often discarded, but that rarely occurs during normal business operations due to more demanding work. In some sense, a business disruption can be good for those small business functions and processes as they may be reworked or revised or simply pared down after a disruption. You may use the process of performing your BIA to recommend paring down these minor business functions as well, though your time is better spent focusing on the mission-critical and vital elements. You may make notes about which functions and processes could be pared down outside of the BC/DR planning process and hand this off to the appropriate SMEs for later action.

From an IT perspective, these types of system outages cause minor disruptions to the business and they can be easily restored. The recovery time requirement for these types of processes often is measured in weeks or perhaps even months.

TIP

Be sure to prompt participants to think about all business processes throughout the year. Some functions and processes occur only during certain times of the year, such as tax season, year end, holidays, and such, and these might be missed during the process. If they're important enough processes, there's a good chance they'll be included, but project management best practices don't rely on luck—they rely on process. Be sure you to ask about any special processes that occur throughout the calendar year that might not immediately come to mind for participants.

Recovery Time Requirements

Related to impact criticality are recovery time requirements. Let's define a few terms here that will make it easier throughout the rest of the analysis to talk in terms of recovery times. As you read through these definitions, you can refer to Figure 4.3 for a representation of the relationship of these elements.

Maximum Tolerable Downtime (MTD). This is just as it sounds—the maximum time a business can tolerate the absence or unavailability of a particular business function. (*Note*: The BCI in the UK uses the phrase Maximum Tolerable Outage (MTO) instead.) Different business functions will have different MTDs. If a business function is categorized as mission-critical, or Category 1, it will likely have the shortest MTD. There is a correlation between the criticality of a business function and its maximum downtime. The higher the criticality, the shorter the maximum tolerable downtime is likely to be. Downtime consists of two elements, the *systems recovery time* and the *work recovery time*. Therefore, MTD = RTO + WRT.

Recovery Time Objective (RTO). The time available to recover disrupted systems and resources (systems recoviery time). It is typically one segment of the MTD. For example, if a critical business process has a three-day MTD, the RTO might be one day (Day 1). This is the time you will have to get systems back up and running. The remaining two days will be used for work recovery (see Work Recovery Time).

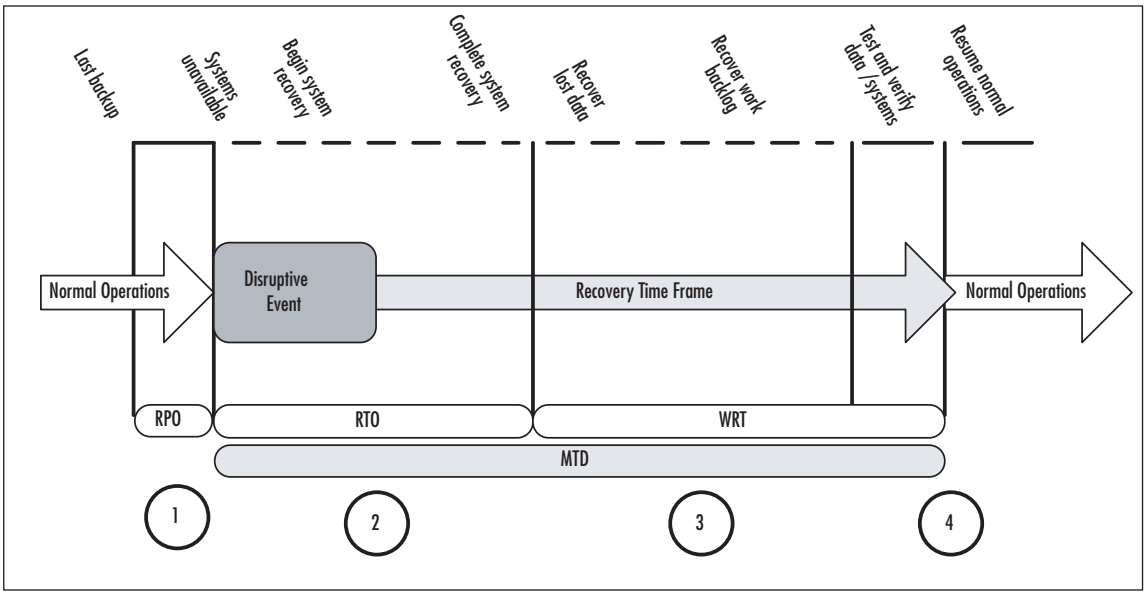
Work Recovery Time (WRT). The second segment that comprises the maximum tolerable downtime (MTD). If your MTD is three days, Day 1 might be your RTO and Days 2 to 3 might be your WRT. It takes time to get critical business functions back up and running once the systems (hardware, software, and configuration) are restored. This is an area that some planners overlook, especially from IT. If the systems are back up and running, they're all set from an IT perspective. From a business function perspective, there are additional steps that must be undertaken before it's back to business. These are critical steps and that time must be built into the MTD. Otherwise, you'll miss your MTD requirements and potentially put your entire business at risk.

Recovery Point Objective (RPO). The amount or extent of data loss that can be tolerated by your critical business systems. For example, some companies perform real-time data backup, some perform hourly or daily backups, some perform weekly backups. If you perform weekly backups, someone made a decision that your company could tolerate the loss of a week's worth of data. If backups are performed on Saturday evenings and a system fails on Saturday afternoon, you've lost the entire week's worth of data. This is the recovery point objective. In this case, the RPO is one week. If this is not acceptable, your current backup processes must be reviewed and revised. The RPO is based both on current operating procedures and your estimates of what might happen in the event of a business disruption. For example, if a tornado touches down in your town and your data center is without power, you may implement your BC/DR plan. If you have an alternate computing location, you may transfer operations to that location. Your next step would be to determine the status of the data. Are you attempting to update systems using backups or were these alternate locations kept up to date? When was the last data

backup performed relative to business operations? What do you need to bring systems up to date? These are the questions you'd need to answer after a business disruption. Therefore, it's important to define your RPO beforehand and ensure your recovery processes address these timelines.

Let's look at how these elements interact. Figure 4.3 graphically depicts the interplay between MTD, RTO, WRT, and RPO. If your company has mission-critical and vital business processes that do not interact with computer systems of any kind, you still need to perform a business impact analysis in order to understand how these manual systems may be impacted by a business disruption, especially natural disasters. At the end of this chapter, we'll walk through an example to help illustrate these concepts. Most companies use technology and computer systems to some extent and the graphic in Figure 4.3 shows how the recovery time is impacted by a business disruption.

Figure 4.3 Critical Recovery Timeframes



- **Point 1**: Recovery Point Objective—The maximum sustainable data loss based on backup schedules and data needs
- **Point 2**: Recovery Time Objective—The duration of time required to bring critical systems back online
- **Point 3**: Work Recovery Time—The duration of time needed to recover lost data (based on RPO) and to enter data resulting from work backlogs (manual data generated during system outage that must be entered)

- **Points 2 and 3**: Maximum Tolerable Downtime—The duration of the RTO plus the WRT.
- **Point 4**: Test, verify, and resume normal operations

During normal operations, there is usually some gap between the last backup performed and the current state of the data. In some operations, this may be minutes or hours; in most organizations it is hours or days. This timeframe is the recovery point objective. In most organizations, this is the same as the period of time between backups. We see at circle 1 that there is a gap showing the point of the last backup and the state of current data, just before the disruption occurs. That's the point at which one or more critical systems becomes unavailable and business continuity and disaster recovery planning activities are initiated. The first phase of the Maximum Tolerable Downtime (MTD) is the recovery time objective. This is the timeframe during which systems are assessed, repaired, replaced, and reconfigured. The RTO ends when systems are back online and data is recovered to the last good backup. The second phase of the MTD then begins.

This is the phase when data is recovered through automated and manual data collection processes. There are two elements of work recovery time. The first is the manual collection and entry of data lost, typically because systems went down between backups. The second phase addresses the backlog of work that may have built up while systems were down. Most companies try to recover the data up to the disruptive event to bring the systems current and then address the backlog, but your business processes may dictate a different recovery order. The key is to understand that there is a delay between the time the systems are back online and the time when normal operations can resume. During the periods indicated by circles 2 and 3, emergency workarounds and manual processes are being used. These are processes that will be developed later in your BC/DR planning process. For example, if a CRM system is down, what processes will your sales, marketing, and customer sales service teams use to interface with and manage customer service delivery? You'll define that in the planning process. Circle 4 indicates the transition from diaster recovery and business continuity back to normal operations. There may be some overlap as manual processes are turned back over to automated processes and you may choose to do it in a rolling fashion—perhaps by department or geographic region.

As you collect your impact data, you'll also need to begin determining the recovery time objectives. You may choose to create a rating system so you can quickly determine recovery time objectives. For example, you might determine that mission-critical business systems or functions should have recovery windows as follows:

- **Category 1**: Mission-Critical—0–12 hours
- **Category 2**: Vital—13–24 hours
- **Category 3**: Important—1–3 days
- **Category 4**: Minor—more than 3 days

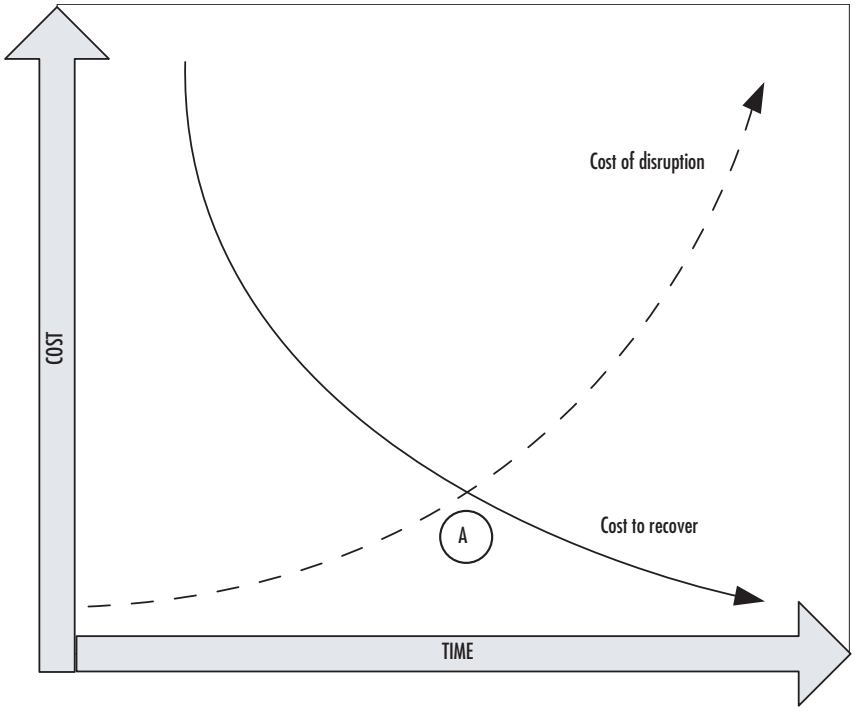
You and your team, with input from the subject matter experts, can determine the appropriate maximum tolerable downtime (MTD) requirements. For some companies, a mission-critical business function could have an MTD of a week. For others, it might be 0 to 2 hours. There is an inverse correlation between the amount of time you can tolerate an outage and the cost of setting up systems that allow you to recover in that time frame. If you can't afford much downtime, you'll clearly have to invest more in preventing downtime and in having systems in place that allow fast recovery times. If you're a small company and can afford a longer MTD, you can spend less on preventing or recovering from outages.

Let's look at an example. In a small company, you may very well be able to do without even mission-critical systems for a couple of days or a week if you really had to. It's possible that you contract with an outside IT service provider to maintain, troubleshoot, and repair your computer systems. If you want a guaranteed two-hour response time, your monthly maintenance costs will be significantly higher than if you sign up for a guaranteed next business day response. So, if you really can't afford to be without that mission-critical business function for more than about eight hours (two-hour response time, six-hour repair time), you'll have to pay more to your service company and you'll probably also have to purchase additional computer equipment to provide some redundancy to prevent extended downtime. These costs add up and the less disruption your business can afford, the more it will cost you to prevent or mitigate those risks. We'll discuss this in more detail in Chapter 5, but it's within the business impact analysis segment where you have to begin making these kinds of assessments.

It's important to note during your impact analysis and subsequent mitigation planning phases that there is an optimal recovery point. Figure 4.4 shows the inverse relationship between the cost of disruption and the cost of recovery. Earlier in this book, we discussed the fact that any business continuity and disaster recovery plan had to be tailored to the unique needs and constraints of the organization. This is particularly true when it comes to the financial costs involved with disruption and recovery.

You can see that the longer you allow a disruption to go on, the more expensive it becomes to the business. Conversely, the longer you have to recover, the less expensive recovery itself becomes. This makes sense when you understand that the longer a business disruption goes on, the more lost revenues, lost sales, and lost customers you accumulate. At the same time, if you need to recover your systems immediately, it's going to cost more to implement things such as zero downtime solutions and hot sites. If you can afford to take a bit more time to recover you have more options, and these options are typically less expensive. If you start plotting these points, you will find an optimal point between these two costs, shown in Figure 4.4 by point A. Each company's intersecting points (point A) will be different based on your company's financial constraints and operating requirements.

Figure 4.4 Optimal Balance between Cost of Disruption and Cost of Recovery



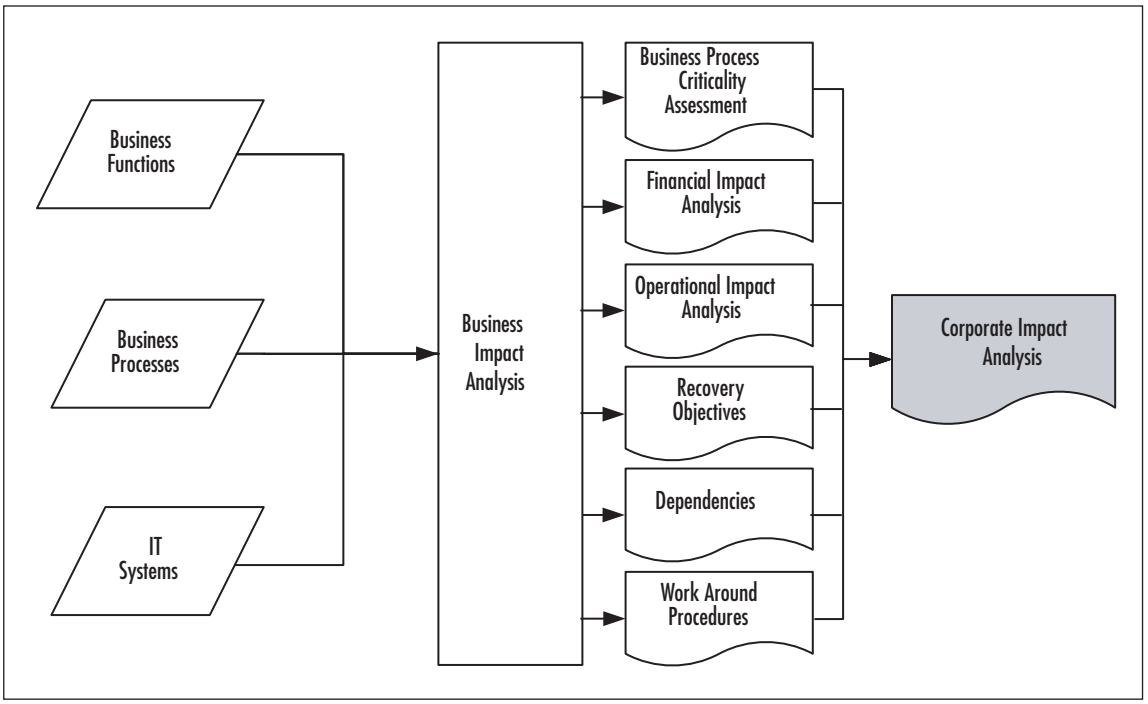
Looking Ahead…

Making the Business Case Makes Your Life Easier

During the assessment and implementation of IT systems over the course of the past few years, you may already have addressed (and invested in) some of the elements needed to reduce the time to recover or to reduce the cost of a disruption. If so, be sure to make note of these systems or investments and be sure to include them in your planning. One way to help make the business case for continued investment is to show how the systems already implemented have made an impact or have contributed to your BC/DR plan. For example, suppose you implemented a mirrored site to allow users to gain access to key data more quickly. That mirrored site also serves as a backup and reduces the cost of disruption to a single site. It also reduces the amount of time it takes to recover, thereby pulling your point A down and to the left (toward lower cost, less time). This investment, then, has contributed to optimizing your balance between cost of disruption and cost to recover while also improving user productivity. Being able to establish and articulate these kinds of IT benefits within your organization may not only win support for your BC/DR plan, it might also help you move up the corporate ladder.

Next, let's look at what the entire analysis process looks like, as shown in Figure 4.5. After we explore this, we'll take a look at the specific data required for inputs and outputs to this process.

Figure 4.5 BIA Inputs and Outputs



In this segment of BC/DR planning, we're looking at business functions, processes, and IT systems to determine criticality. Business functions can be defined as activities such as sales, marketing, or manufacturing. Business processes can be defined as how those activities occur. Are your sales conducted via a Web site, via telephone, via sales calls? How are orders processed? How are employees hired? These are business processes, they describe how the functions get done. By first identifying business functions, you then can focus on the key processes in each function to develop a comprehensive view of your company. The third input area, shown in Figure 4.5, is IT systems. In most companies, the business processes are carried out in part through computer systems, applications, and other automated systems. Identifying mission-critical business functions and processes and how they intersect with IT systems will help you map out your business continuity and disaster recovery strategies.

Once you have compiled that data, you'll perform the analysis to generate the needed outputs, including the criticality assessment, the impact assessments (financial and operational), required recovery objectives, dependencies, and work-around procedures. The work-around procedures will enable you to get critical business functions back up and running as

quickly as possible. These work-around procedures may be used during the RTO and WRT periods discussed earlier and shown in Figure 4.3. As you can see, the output is a comprehensive corporate impact analysis. This is the same output shown in Figure 4.2 and is the end of the larger risk assessment phase in our overall BC/DR planning process. The impact analysis will be used as input to the risk mitigation planning segment of the BC/DR project and we'll discuss that in Chapter 5.

Identifying Business Functions

In this section, we're going to walk through some of the more common business functions found in business today. It's not a comprehensive list but it's intended to do two things. First, you can include these in your BIA and you'll know you've got the major items covered. Second, you can use this to spur your thinking to include other areas that might be related to the items listed. You should begin by listing all the business functions that come to mind unless it's clear they should *not* be included. As with your risk assessment, it's best to begin by scanning the wide horizon and narrowing your focus later on. It's always easier to cut than to try to find gaps later.

When possible, it's advisable to create a list of all the functional areas of the business and gather SMEs from each area to discuss the critical business functions. Although it's more time consuming to get everyone in a room together, you will more quickly discover interdependencies in this manner. If SMEs sit quietly by themselves and come up with the critical business functions alone, they might miss the elements that are vital to other areas. An alternate method of gathering this data is to have the SMEs generate a list of questions to ask others in their area and compile the results. When the compiled results are ready, the subject matter experts from all areas of the company can meet to go over the results with the specific mission of finding interdependencies. How you manage this aspect of the project will have everything to do with how your company runs on a day-to-day basis.

The common business functions include those shown here. They're listed in alphabetical order, not necessarily in the order in which you would review these areas. The order in which these are reviewed will be dictated by the project management processes you've defined, the data gathering methods you choose, and the structure of your company. Following this section, we'll discuss the specific data points you need to gather from each of these areas.

1. Facilities and Security
2. Finance
3. Human Resources
4. Information Technology
5. Legal/Compliance

6. Manufacturing (Assembly)
7. Marketing and Sales
8. Operations
9. Research and Development
10. Warehouse (Inventory, Order Fulfillment, Shipping, Receiving)

As we look at these business functions, keep your business in mind and think about the key processes that occur in each functional area. After you've documented your key business processes, you will assign a criticality rating to them similar to the ones discussed earlier. As a reminder, you may also want to document key positions, skills, and knowledge in these functional areas. For example, what would the impact be if your head of facilities was injured in a building collapse and your company needed to operate from an alternate location? Who would head that up? What skills or knowledge would be needed in order to temporarily (or permanently) replace your facilities manager in the aftermath of a business disruption? These human factors should be assessed in conjunction with the major business functions.

Facilities and Security

Your company may be located in a single office in a small office building or it may span several continents. Regardless of how many physical locations your company operates, you need to understand the critical processes performed by facilities and security management with regard to your business operations. If a business disruption were to occur, what processes and procedures would be needed in order to get your business back up and running? For example, if the building is damaged or destroyed, physical security of the building will be disrupted. Employees won't be able to just swipe their badge at the front door. Is this a critical business function or not? It depends. If the building is destroyed, it doesn't matter that they can't get into the building. You don't just need an alternate process, you need an alternate location. Once an alternate location is established, you need facilities support. So, the critical business function, in this example, is having a place of business ("facilities"). Security and access are secondary. Notice how it helped to think of a specific scenario—it focused our thinking so we could see the key areas. Is having a place of business a critical business function? Not in the formal definition of a business *process*, but it's certainly important. Security usually involves a process—adding employees to access lists, providing employees with badges, IDs, or other identification, and granting them appropriate access to company resources. This might be highly important during normal business functioning, but does it impact the company's mission-critical operations? It depends on your business. If you work in a secure research environment, facilities and security may be mission-critical. If you work in a software development firm where employees could check code out of an online library and work from home, facilities and security may not be mission-critical at all. Facilities and security, though, may have some critical business functions beyond these macro-level func-

tions just mentioned. For example, is facilities involved with the receiving or shipping of products, inventory, or other tangible goods? If so, these may be critical business functions to be included.

Finance

By definition, the financial workings of the company are critical business functions, but not all financial functions are mission-critical functions. For example, tracking receivables and payables are critical business functions because without the ability to keep track of what others owe you and what you owe others, you have no idea about the financial status of the company. Employee payroll is another critical business function (which is a financial transaction that might fall under the purview of the Human Resources department). If employees are not paid, if appropriate withholding and other taxes and deductions are not taken, your company faces serious problems, with employees and with state and federal authorities.

If your company has legal obligations to pay back a loan from a bank or make payments or reports to investors, these also might be critical business functions to be included in your analysis. In some cases, you may have some leeway with regard to repayment if you experience a natural disaster, but don't count on it. Your financiers don't care, they just want payments on time and in full. Therefore, keeping track of these kinds of financial and legal obligations may be considered critical business functions, depending on the nature of your company and its financing structure.

Accounting, finance, and reporting functions within finance should be reviewed and analyzed. There are many interdependencies in financial functions that cross over into HR, marketing, sales, IT, and operations. If key IT systems were to go down, which business processes would be impacted? Which processes and functions would have to get back up and running first in order to keep the business going?

Human Resources

If your firm experiences some sort of natural disaster, your Human Resources staff will be busy trying to fulfill a number of roles. Employees will usually contact HR for information on the status of the building, the status of the company, whether they should report to work, where they should report to work, and so on. Employees may also use HR as a clearing house for information about the well-being of other employees or information on the broader community. Finally, employees will be looking to HR for information on how, when, and where they'll get paid. In fact, this will likely be the first question many employees ask, especially if the business disruption happens just prior to or on payday. The staff in HR will be in the best position to provide guidance on the kinds of issues for which employees come to them. From there, you can compile a list of critical business functions. Remember, create a list of all business functions, then prioritize them later. If IT systems were to go down, which HR functions and processes are mission-critical? How would they

be accomplished in the absence of IT systems? How would this impact other areas of the company?

IT

Critical business functions for IT? It seems like almost all of them are critical most of the time, especially if you judge by the phone calls, hallways pleas, and e-mails begging for assistance when one of the applications, servers, or hardware goes down. However, ultimately, the hardware and software should support the critical business functions, so the IT functions, in large part, will be driven by all the other departments. HR might say "we have to have our payroll application"; marketing might say "without our CRM system, we can't sell any products"; manufacturing might say "without our automated inventory management system, we can't even begin to make anything." Therefore, the IT department's critical business functions are driven externally, to a large degree. However, there are also business functions that occur within the IT department critical to the company's ability to recover and continue doing business after a disaster. For example, the IT department needs to create backups of all data that changes after a disaster. If a disaster happens on a Tuesday and you're able to get some systems back up and running by the following Monday, backups need to start on Monday, as soon as data begins being generated, saved, or changed. Therefore, backup processes can be viewed as critical business functions from the IT perspective. Managing security is another critical aspect. As you look at these functions, you'll find addtional critical IT functions.

Legal/Compliance

There are numerous mission-critical business functions related to legal and compliance areas of your company. If your firm is subject to legal or regulatory statutes and requirements, you're already well aware of these constraints. You need to view these constraints and requirements in light of a potential business outage to determine which of these are mission-critical, which are vital or important, and which are minor in nature. For example, if your firm deals with private or confidential personal data, it must be protected at all times, even if you move to a manual system for the duration of a system outage. Which systems, then, should be recovered first? Which business processes are mission-critical? Those related to remaining in compliance, both in terms of business process and business data, should be ranked very high on your list. The legal and financial consequences, as discussed in the case study earlier in this book (see Case Study 1, "Legal Obligations Regarding Data Security") can be enormous.

Manufacturing (Assembly)

If your company is involved with the manufacturing, assembly, or production of tangible products, you obviously need to scour this area for mission-critical functions since your ability to produce your products is the engine that drives your company. There may be some systems that can come online later, but there are likely to be certain systems that must be up and

running in order for any manufacturing, assembly, or production to occur. Identify these business processes and systems by understanding what would happen if the production equipment were to be damaged or destroyed. Next, understand what would happen if the production equipment was left in tact but upstream or downstream events impacted your customers or vendors. The impact analysis needs to include both internal and external elements. What business processes should you put in place to deal with the potential loss of a key supplier? We'll look at risk mitigation strategies in detail in Chapter 5. For now, you should be identifying the potential impact of various business disruptions to your manufacturing operations, keeping both internal and external (upstream/downstream) disruptions in mind.

It's also important to understand the interaction between any manufacturing/assembly automation equipment and IT systems. If IT systems go down, how are automation systems impacted? If automation systems go down, how are IT systems impacted? What manual processes can be implemented in the absence of either automation systems or associated IT systems?

Marketing and Sales

Marketing activities help create demand for the company's products and services by establishing or expanding knowledge of the company and its products/services. Sales activities are those actions that actually create a sales transaction and bring revenue into the company. Some companies may determine that marketing activities in the aftermath of a business disruption can be put on hold while sales activities should be a top priority. Other companies may see marketing activities as mission-critical in the aftermath of a business disruption because they are businesses that need to stay in touch with customers, keep their products/services in front of customers, and cannot afford to let rumors and erroneous information about the company's status float around, especially in today's world of instant, on-demand news. How you approach marketing and sales functions in your firm from a business continuity and disaster recovery standpoint will depend largely on the size of your company, its market visibility and other internal factors. Clearly activities that support the company's ability to perform sales transactions will most often be considered either vital or mission-critical activities and systems.

Operations

If your company doesn't manufacture, assemble, or produce tangible products, it probably develops and sells intangible products such as service, software development, research, analysis, and others. Whatever it is your company does, it sells something in order to generate revenue. Therefore, your operations are what end up generating those goods and services that are sold to customers. As with manufacturing and assembly, operations are what generate sales and therefore are almost always part of the most urgent mission-critical business functions. Although "operations" is a rather broad and vague term, each company knows exactly

what its operations are and how these operations contribute to revenue generation. It is within that scope of knowledge that these activities should be assessed for criticality.

Research and Development

Some companies or organizations are funded through investors, through grants, or operate as nonprofits. They may be dedicated solely to research and development and may not generate revenue in the traditional sense of the word. However, every organization needs funding and that funding almost always comes with some sort of expectations and requirements about what is to be achieved with that funding. Therefore, you can view activities that bring in funding as your sales activities and can assess their criticality in that light. For example, if your organization does biochemical research and you're funded by federal or state programs, you still have business functions related to deliverables to consider. Is the next round of funding predicated upon the successful delivery of the results of current development or testing? If so, you have several mission-critical systems to consider along with assessing the impact of a business disruption to your research. Do you have live cultures growing in a lab that need to be tested and assessed? If so, what would happen if the research building was destroyed by fire or by an earthquake or tornado? How would your research be impacted and how would you recover? Though these are a bit different from traditional business functions and are not related directly to IT systems, these are questions that should be asked and answered if you're in this business.

Warehouse (Inventory, Order Fulfillment, Shipping, Receiving)

If your company deals in tangible goods of any kind, you have processes for handling inventory, order fulfillment, returns, shipping, and receiving. In some companies, these functions are handled by outside firms. For example, you may manufacture or assemble a product that is sent out daily on trucks to some other company that handles the remaining inventory processes. Nonetheless, your company has to keep track of what it makes and what it ships out at minimum. So, there are two elements here, the actual manufacturing or assembly (covered earlier) and the tracking, storing, and moving of these products. These two functional areas are closely tied together and the interdependencies in these areas should be given special attention. If IT systems go down, how are these activities impacted? If the building is ravaged by fire or flood, how are these activities impacted?

Other Areas

There may be other functional areas not listed here that exist in your company. If so, be sure to explore each functional area and determine the various business processes used in each area along with their relationship to the business's IT systems.

Looking Ahead…

Flaws Exposed

It's important to understand that a business impact analysis is a thorough business assessment that involves an unbiased study of the entire organization. When you start looking at the workings of the company in a very close and detailed manner, things may start to look less than stellar, like when you shine a very bright light on something and you suddenly see all its flaws quite clearly. Your corporate executives might take one of two positions. In the best case, they will appreciate the opportunity to closely examine the company's operations and find ways to improve it along the way. In the worst case, they will hesitate, stonewall, or misdirect you in order to prevent you from uncovering business processes that are broken, inefficient, or worse, illegal. So, be prepared for a variety of reactions from the top to the bottom of your organization. Also, if you're so inclined, you might begin preparing your organization for this level of scrutiny, being sure to communicate the positive aspects of this process.

Ideally, you can double your mileage from this project by using it as an opportunity to perform your BIA and to streamline business operations. Just be prepared for a few bumps in this road, especially if you suspect that the business processes are not too pretty in some areas of the company. Remember, too, that a well-executed BIA can help you garner *more* support for your BC/DR planning project as people in the organization begin to understand the undesirable effects a disaster or disruption would have on the business. Sometimes seeing the flaws is motivation enough to fix them.

Gathering Data for the Business Impact Analysis

As we discussed in Chapter 3, there are four primary ways of gathering information: questionnaires, interviews, documents, and research. This holds true for the BIA as well. Before you can develop questionnaires or interviews, however, you have to know what you're looking for. You may choose to gather subject matter experts who then create questionnaires or interview questions. As a project team, you may create a number of very specific questions or scenarios to be presented to subject matter experts (SME) in the form of questionnaires or interviews. The additional information will come from either the project team or SMEs reviewing documents or performing targeted research.

Where to start this sometimes daunting process? One of the best places to start is with your company's organizational chart. Lacking that, try the company's phone directory—electronic or paper. In many cases, the functional areas of the company are clearly spelled out.

This can be a good place to determine sources for subject matter experts as well. You can begin by creating a list of each functional area such as each division or each major work area such as manufacturing, warehouse, operations, development, among others. List subdepartments or subdivisions under each of the major headings, as appropriate. Now, you should have a comprehensive list of the major and minor departments, which are often the functional areas, in your company. Check for duplication and remove any areas that are repeated or that clearly should not be included. The key at this juncture is to generate a comprehensive list of business functions that can later be prioritized. Also remember there may be internal or external dependencies that raise the criticality of particular business functions.

As previously discussed, asking questions and providing scenarios to consider can help people focus on specific business issues and generate better responses. Some questions you might ask of your subject matter experts to help them focus on the key aspects of the impact analysis include these:

1. How would the department function if desktops, laptops, servers, e-mail, and Internet access were not available?
2. What single points of failure exist? What, if any, risk controls or risk management systems are currently in place?
3. What are the critical outsourced relationships and dependencies? What are the upstream and downstream risks to your business function?
4. If a business disruption occurred, what workarounds would you use for your key business processes?
5. What is the minimum number of staff you would need and what functions would they need to carry out?
6. What are the key skills, knowledge, or expertise needed to recover? What are the key roles that must be present for the business to operate?
7. What critical security or operational controls are needed if systems are down?
8. How would this business function in a backup recovery site? What would be needed in terms of staff, equipment, supplies, communications, processes, and procedures? (This crosses into the disaster recovery element, which we'll discuss more in a later chapter.)

Data Collection Methodologies

For the business impact analysis, it is advisable to collect data through questionnaires, interviews, or workshops, which are in many ways group interviews. Additional data can be gathered using documents and research, but this data should be gathered only to support or supplement data gathered through direct contact with business subject matter experts. The

reason for this is fairly obvious. Only those who actually perform various business functions can assess the criticality of those business functions. You could sit down and read documents all day long and never get a clear picture of what's really mission-critical and what's just important. Therefore, you should rely primarily on questionnaires, interviews, and workshops for this segment of your data gathering. Let's look at methodologies you can use for these three data gathering methods.

Questionnaires

Questionnaires can be used to gather data from subject matter experts (SME) in a fairly efficient manner. Though it takes time to develop a highly useful questionnaire, SME's responses will be consistent, focused, and concise. They can fill out the questionnaires regarding their business units, business functions, and business processes at a time that is convenient for them (within a specified timeframe), thereby increasing the likelihood of participation. On the downside, questionnaires that are sent out may be ignored, pushed aside, or forgotten. In order to generate a timely and meaningful response to your team's questionnaire, you can create a methodology that will increase your response rate.

First, it's important to appropriately design the questionnaire. If it's full of useless questions, if it's visually confusing or overwhelming, you'll decrease your response rate. The questionnaire should be clear, concise, easy to understand, and fast to fill out. If you want to use a Web-based questionnaire that records data in a database, so much the better. You can send out reminders with a link to the questionnaire as frequently as needed. With a paper-based questionnaire, there's a lot of moving of paper and the increased likelihood that the paper will be misplaced, lost in a pile, or simply thrown out.

It's also important to explain the purpose of the questionnaire to the participants in a manner that helps them buy into the process. Focus on what's in it for them, not for you. They probably don't care that *you* need this data, but they will care that this data could help prevent some problem in *their* jobs. Ideally, you should hold a kick off meeting where the questionnaire is introduced and explained, the purpose of it is clearly articulated, and the process for completing the questionnaire is explained. For example, you might let people know that the questionnaire is available at a particular location, that it takes a total of three hours to complete per department, but that it can be completed in segments and the questionnaire-in-progress can be saved for later completion. You should let people know who the contact person is if they run into problems and when the questionnaire must be completed.

If your company is the type of company that likes to have a bit of fun in these kinds of meetings, you can also announce small prizes that will be awarded to departments or individuals who complete theirs correctly first, who are most thorough, and so forth. Be careful, though, you don't want to leave the impression that this is a race to the finish (where important details can be lost) or that "cute" answers are appropriate. You can, however, announce that for any SME that submits a complete and thorough questionnaire by the deadline will be entered into a hat for the chance to win some prize such as a portable

music player, a new cell phone, dinner for two at a nice restaurant, among others. Sometimes small incentives to do the right thing can go a long way in getting people to participate in the manner expected and needed. Considering how vital this particular data is to your entire BC/DR plan, it's usually worth a small investment to get people to participate appropriately, if this type of activity fits in with your corporate culture. Be sure to provide information on how respondents can get assistance with the questionnaire—either from a technical standpoint (if it's an electronic or Web-based questionnaire) or an administrative standpoint. If they don't understand exactly what a question means, who should they contact? How should they contact them? What is the contact person's e-mail, location, phone number, and work hours? Be sure to provide this information so you don't inadvertently create roadblocks for yourself.

Finally, let the team know how they'll learn about the results of the questionnaire. Most people dislike spending time filling out a form only to never hear about it again. If they are willing to take the time needed to provide this data, there should be some reciprocity. For example, if this data is all pumped into a database, a report on each respondent's data could be provided back to them for verification. Once the data is reviewed by your team, there may be additional questions. Respondents should be told, in advance, about the process for following up with them regarding their responses to the questionnaire.

Once questionnaires are completed, you and your team should review them to ensure they are complete. In some cases, you may choose to create a process whereby certain questionnaires are followed up by an interview. This might be in the case of the most critical business functions or where questionnaire data indicates there may be confusion, conflict, or incomplete data. Any follow-up interviews should follow a specific format as well so that targeted data can be collected.

Interviews

If your team has decided that data will be gathered through interviews, you'll still need to create a questionnaire type of document that will provide the interviewers with a set of questions to which they gather responses. Free form or informal interviews will yield inconsistent data across the organization and you'll have a wide array of meaningless data. Develop a questionnaire and use it as the basis of the interview process. Each interview should follow a predefined format and the questions asked of each respondent should be the same. Develop a questionnaire, interview, or question sheet from which the interviewer will work and also develop a corresponding data sheet onto which the interviewer can record responses. Look to find methods to speed up the interview process. For example, don't use a rating system of ten elements that use 1 as NEVER and 10 as ALWAYS with eight other word/number combinations. This will be cumbersome for the interviewer to describe and will be almost impossible for the interviewee to remember. If you choose, you might say, "On a scale of 1 to 10 with 1 being never and 10 being always, how often would you say you access the CRM database on a telephone sales call?" This sort of sliding scale can be

used because the respondent does not have to remember 10 different descriptions—what does three mean again? However, the danger is that each respondent is going to give you a different sliding scale number if the range is 10. Instead, you might use a three-element scale without numbers. "How often do you use this system during a telephone sales call? Never, sometimes, or always?" That's much easier for the respondent to remember and evaluate and it's also more likely to generate a more consistent response across all respondents.

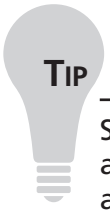
Our goal is not to go into the pros and cons of various data gathering methods, but to point out that there are unintentional problems you can build into a questionnaire or survey that can skew your results. If your organization has a group that develops market surveys or questionnaires, you may ask them to review your questionnaire before rolling it out. They might spot something you missed and help you gather better data. We all know the output is only as good as the input, so making sure your data gathering methods are clean will help on the other side of this assessment process.

Once an interview is conducted, the data needs to be reviewed and verified by the interviewee. Due to the nature of an interview, it's possible one of the people (interviewer, interviewee) misunderstood the question or response. Therefore, once the data is prepared, it should be reviewed by the interviewee before being finalized. You want to avoid having the interviewee rehash their previous responses, but you do want to provide an opportunity for additional insights and information that clarify previous responses. Follow-up interviews, if needed for clarification, should be scheduled as quickly after the initial interview as possible so that the data, response, and topic are still fresh in the interviewee's mind.

Workshops

Data collection workshops can be an effective method of gathering needed data. If you choose this method of gathering data, you might still choose to create a questionnaire so that you can be sure you cover all the required data points. Identify the appropriate level of participating personnel and gain agreement as to participants. Choose an appropriate time and place for the workshop, ensure the appropriate amenities will be available (white boards, refreshments, etc.). Develop a clear agenda for the meeting and distribute this, in advance, to meeting participants. Identify the workshop facilitator and clearly define his or her role in the process. Identify workshop completion criteria so the facilitator and participants are clear about what is expected, what the required outcomes are, and how the workshop will conclude. The facilitator's job is to ensure the workshop objectives are met, so these objectives must be clearly articulated prior to the start of the workshop. Develop or utilize an appropriate process for dealing with issues during the workshop so that participants stay on topic and focused on the key objectives. Some companies use the concept of a "parking lot," where issues are written up on note cards and collected or written on sticky notes and posted on a white board or an empty wall. Use an issue tracking methodology that allows you to stay on topic but make note of issues. Also identify the method you'll use for addressing those issues that cannot be (or should not be) resolved during the course of the

workshop. Finally, ensure that the results of the workshop are written and well documented and that participants have the opportunity to review the results for errors and omissions before they are finalized.



TIP

Select the format for data gathering that is least intrusive on people's time and that is most aligned with how you normally work. Business continuity and disaster recovery planning are often very low on people's priorities and anything you can do to reduce the effort it takes to provide the data you need will pay off.

Determining the Impact

We've delineated some of the more common business functions. Now, let's turn our attention to some of the specific impacts to a business. As with other lists, this one is extensive but not necessarily exhaustive. Be sure to review this list and remove any items that do not pertain to your business and add any elements that are not included that do relate to your business. Remember, too, that a business disruption can run that gamut from a hard drive failure to an earthquake that levels your building to a pandemic that impacts an entire region or nation. Once you've looked at all the potential impact points, we'll discuss specific data points to collect and analyze as well as how to put those together with your risk assessment data. The impact of any business disruption may include:

1. **Financial**. Loss of revenues, higher costs, potential legal liabilities with financial penalties.
2. **Customers and suppliers**. You may lose customers and suppliers due to your company's problems or you may lose customers or suppliers if they experience a business disruption or disaster.
3. **Employees and staff**. You may lose staff from death, injury, stress, or a decision to leave the firm in the aftermath of a significant business disruption or natural disaster. What are the key roles, positions, knowledge, skills, and expertise needed?
4. **Public relations and credibility**. Companies that experience business disruptions due to IT systems failures (lost or stolen data, modified data, inability to operate due to missing or corrupt data, etc.) have a serious public relations challenge in front of them. These kinds of failures require a well-thought-out PR plan to help support business credibility. What impact would system outages or data losses have on your public image?

5. **Legal**. Regulations regarding worker health and safety, data privacy and security, and other legal constraints need to be assessed.
6. **Regulatory requirements**. You may be unable to meet minimum regulatory requirements in the event of certain business disruptions. You need to fully understand these regulations and their requirements related to business disruptions, both natural and man-made.
7. **Environmental**. Some companies may face environmental challenges if they experience failures of certain systems. Understanding the environmental impact of system and business failures is part of the business impact analysis phase.
8. **Operational**. Clearly operations are impacted by any business disruptions. These must be identified and ranked in terms of criticality.
9. **Human Resources**. How will staff be impacted by minor and major business disruptions? What is the impact of personnel responses to business operations? What are the qualitative issues to be addressed (morale, confidence, etc.)?
10. **Loss Exposure**. What types of losses will your company face? These include property loss, revenue loss, fines, cash flow, accounts receivable, accounts payable.
11. **Social and corporate image** (strongly tied to public relations). How will employees, customers, suppliers, partners, and the community view your company? How will its image be altered by a minor or major business disruption?
12. **Financial community credibility**. How will banks, investors, or other creditors respond to a minor or major business disruption? If the cause is a natural disaster, the challenges are different than if the cause is man-made. If the company failed to secure or protect data or resources, there are additional consequences both to the corporate image and to the company's credibility in the marketplace.

(Adapted from the Disaster Recovery Institute)

After you've compiled a list of your business functions and processes, you should assign a criticality rating to them. Payroll, accounts payable, and accounts receivable usually qualify as mission-critical business processes. Furniture requisitions for new employees usually fall to the bottom of the list as minor. Rate all your identified business processes and sort them in order of criticality. You might end up with a table or matrix that looks something like that shown in Table 4.1.

Table 4.1 Business Function and Criticality Matrix

Business Function	Business Process	Criticality
Human Resources	Payroll	Mission-critical
	Employee background checks	Important
Finance	Debt payments/loan servicing	Vital
	Accounts receivable	Mission-critical
	Accounts payable	Mission-critical
	Quarterly tax filings	Mission-critical
Marketing and Sales	Customer sales calls	Mission-critical
	Customer purchase history analysis	Vital

Business Impact Analysis Data Points

The number and type of data points you collect in your business impact analysis is largely a function of the size and type of company in which you work. Smaller companies will have fewer data points, larger companies will have more. However, you can also inundate yourself with too many data points if you don't take a focused approach. Some companies are extremely slow moving, analytical types of companies in which all data must be collected and assessed. Other companies move at the speed of light (typical in start ups) and want to grab just the high points and move on. The plan you devise needs to find a balance between information overload and superficial data. Be sure to include enough detail so that you can actually develop strategies that will help your company survive a serious business disruption, but don't allow the information floodgates to open and overwhelm you with minutiae.

Table 4.2 shows various data points you can consider collecting along with a brief description of the purpose or focus of that data point. Feel free to modify this to suit your unique needs.

Table 4.2 Business Impact Analysis Data Points

Data Point	Description	IT Dependencies
Business function or process	Short description of the business function or process (we'll use "function" from here on).	Describe primary IT systems used for this business function.

Continued

Table 4.2 continued Business Impact Analysis Data Points

Data Point	Description	IT Dependencies
Dependencies	Description of the dependencies to this function. What are the input and output points to this function? What has to happen or be available in order for this function to occur? What input is received, either from internal or external sources, that is required to perform this business function? How would the disruption of this business function impact other parts of the business? How and when would this disruption to other functions occur?	Describe IT systems that impact or are impacted by this business function. Are there any internal or external IT dependencies?
Resource dependencies	Is this business function dependent upon any key job functions? If so, which and to what extent? Is this business function dependent upon any unique resources? If so, what and to what extent (contractors, special equipment, etc.)?	Describe secondary/support computer/IT systems required for this business function to occur.
Personnel dependencies	Is this function dependent on specialized skill, knowledge or expertise? What are the key positions or roles associated with this function? What would happen if people in these role were unavailable?	Describe key roles, positions, knowledge, expertise, experience, certification needed to work with this particular IT system or IT/business function.
Impact profile	When does this function occur? Is it hourly, daily, quarterly, seasonally? Is there a specific time of day/week/year that this function is more at risk? If there a specific time at which the business is more at risk if this function does not occur (tax time, payroll periods, year end inventory, etc.)?	Describe the critical timeline related to this function/process and related IT systems, if any.

Continued

Table 4.2 continued Business Impact Analysis Data Points

Data Point	Description	IT Dependencies
Operational	If this function did not occur, when and how would it impact the business? Would the impact be on time or recurring? Describe the operational impact of this function not occurring.	Describe the impact on IT if this business function does not occur. Describe the impact on operations if this business function does not occur.
Financial	If this function did not occur, what would be the financial impact to the business? When would the financial impact be felt or noticed? Would it be one time or recurring? Describe the financial impact of this function not occurring.	
Backlog	At what point would work become backlogged?	Describe how a backlog would impact IT systems and other related or support systems.
Recovery	What types of resources would be needed to support the function? How many resources would be needed and in what timeframe (phones, desks, computers, printers, etc.)?	What resources, skills, and knowledge would be required to recover IT systems related to this business function?
Time to recover	What is the minimum time needed to recover this business function if disrupted? What is the maximum time this business function could be unavailable?	How long would it take to recover, restore, replace, or reconfigure IT systems related to this business function?
Service Level Agreements	Are there any service level agreements in place related to this business function? What are the requirements and metrics associated with these SLAs? How will SLAs be impacted by the disruption of this business function?	How would IT service levels be impacted by the disruption or lack of availability of this business function? How do external SLAs impact IT systems?

Continued

Table 4.2 continued Business Impact Analysis Data Points

Data Point	Description	IT Dependencies
Technology	What hardware, software, applications, or other technological components are needed to support this function? What would happen if some of these components were not available? What would be the impact? How severely would the business function be impacted?	What IT assets are required to support/maintain this business function?
Desktops, laptops, workstations	Does this business function require the use of "user" computer equipment?	What is the configuration data for required computer equipment?
Servers, networks, Internet	Does this business function require the use of back-end computer equipment? Does it require connection to the network? Does it require access to or use of the Internet or other communications?	What is the configuration data for required servers and infrastructure equipment?
Work-arounds	Are there any manual work-around procedures that have been developed and tested? Would these enable the business function to be performed in the event of IT or systems failures? How long could these functions operate in manual or work-around mode? If no procedures have been developed, does it seem feasible to develop such procedures?	Are there any IT-related work-arounds related to this business function? If so, what are they and how could they be implemented?
Remote work	Can this business function be performed remotely, either from another business location or by employees working from home or other off-site locations?	Can this business function be performed remotely from an IT perspective? If so, what would it take to enable remote access or the ability to remotely perform this business function?

Continued

Table 4.2 continued Business Impact Analysis Data Points

Data Point	Description	IT Dependencies
Workload shifting	Is it possible to shift this business function to another business unit that might not be impacted by the disruption? If so, what processes and procedures are in place or are needed to enable that function?	Are there other IT systems or resources that could pick up the load should a serious disruption occur?
Business/data records	Where are the business records related to this function stored or archived? Are they currently backed up? If so, how, with what frequency, where?	How and where are backups stored? Based on data provided, is the current backup strategy optimal based on the risks and impact?
Reporting	Are there legal or regulatory reporting requirements of this business function? If so, what is the impact of a disruption of this business function to reporting requirements? Are there reporting work-arounds in place or could they be developed and implemented?	Are there other ways reporting data could be generated, stored, or reported if key business functions or systems were disabled?
Business disruption experience	Has this business function ever been disrupted before? If so, what was the disruption and what was the outcome? What was learned from this event that can be incorporated into this planning effort?	Has IT ever experienced the disruption of this business function in the past? If so, what was the nature and duration of the disruption? How was it addressed and what was learned from the event?
Competitive impact	What, if any, is the competitive impact to the company if this business function is disrupted? What would the impact be, when would the impact occur, when would the potential loss of customers or suppliers occur?	

Continued

Table 4.2 continued Business Impact Analysis Data Points

Data Point	Description	IT Dependencies
Other issues	What other issues might be relevant when discussing this particular business function?	Are there other IT issues related to this specific business function that should be included or discussed?

Once you've collected all these data points for all your business functions and processes, you have a comprehensive understanding of your business, its key functions, and what would happen if those functions were disrupted. In the next chapter, we'll discuss how to develop risk mitigation strategies based both on the various risks your company faces and on the criticality of the various business functions as defined in this phase of the assessment.

Common Challenges…

Data Overload

The difficulty with the business impact analysis is that it can generate huge volumes of data that need to be sorted, assessed, and analyzed. There is no shortcut to getting this done, but it might help to keep the outcome in mind. The result you're looking for is an analysis of the critical functions and processes used in your company to conduct your company's business. Using the scenario approach can really help you focus in on the end result. If servers go down, if power goes out, if fire rages, if tornados strike, what are the most important things your company needs to accomplish to get business going again? We'll address the disaster recovery elements in an upcoming chapter—the things you need to do to stop the impact of the disruption or emergency before business can resume. For now, you need to understand what is absolutely essential to keep your business running. If you can keep this in mind as you go through this process, you're likely to be able to tune out the irrelevant and extraneous data more effectively.

Understanding IT Impact

As you can see from Table 4.2, the IT functions can be correlated to the business functions and processes at each step. As you gather this data, you will need to continually correlate the business functions/processes with the IT systems used to carry out or facilitate those functions in order to avoid gaps in your planning. In most cases, the subject matter experts and

participants in this analysis will discuss the relationship of the IT systems to these functions. However, it's important to continually look at the intersection of IT systems to these business functions since the SMEs and departmental representatives may not fully understand the interdependencies of data or systems across the enterprise. For example, an SME might understand that use of the CRM system is vital to her job, but she may not have a clue that the CRM system resides on a server on the fourth floor and requires data updates from three other sources. From an IT perspective, you'll see this vital CRM function as a series of servers, applications, and data flows. As you work with the BC/DR team to map out the business functions and processes, you'll need to develop a parallel map of how that information intersects with IT equipment and functions.

In addition, you'll need to develop an understanding of how long it would take to replace or repair IT equipment based on the assessment of criticality. When you move into the risk mitigation phase, you might decide that the most optimal solution is to implement a fully redundant system for three key functions because the replacement or repair time for these systems exceeds the maximum tolerable downtime. The analysis of the data gathered in this phase must include IT-specific data so that you can optimize your risk mitigation strategies (coming up in Chapter 5).

The impact of IT on business functions (and the impact of business functions on IT) is usually already pretty well understood by the IT department through normal IT activities. However, the information gathered in this business impact analysis phase will bring to light new priorities, new gaps, and new challenges to be addressed through the IT department. Understanding how this data impacts IT and how IT impacts this data is key to developing a solid BIA and a comprehensive BC/DR plan.

TIP

You may want to encourage your subject matter experts to include their assessment of the impact on IT systems and the impact of IT systems on their critical business processes. By having them include this data, you can see IT from their perspective. You might learn something new about how they use IT systems or what you can do to mitigate risk to key business processes using IT technologies. At the very least, it will help flesh out your IT impact analysis.

Example of Business Impact Analysis For Small Business

Let's look at an example to help make this entire process a bit more tangible. A company of about 125 employees works out of a single location. They're situated in a light industrial area surrounded by warehouses and wholesalers. They sell a variety of specialty building hardware such as hard-to-find latches, fasteners, locks, and more. They purchase products from a variety of manufacturers and distributors and sell to a niche market in their region. These customers call in orders periodically. They also run a Web site that has seen sales grow significantly in the past three years, so that Web sales are now equal to non-Web sales.

The company, which we'll call ABC Hardware, does about $20 million a year in sales, about half of that online. Their facility is a large space comprised mostly of warehouse space with some office space. They ship and receive packages daily for Web operations and they ship weekly for their non-Web customer orders.

This company's risks include:

- Risk of fire in the building
- Risk of flooding in the area
- Risk of chemical spill in the area
- Risk of upstream/downstream losses by suppliers, vendors, customers

Let's focus on the risk of a fire in the building. If a fire struck the building, the damage might be contained to one of the areas, either warehouse or office. If the warehouse experienced a fire, inventory would be damaged and the ability to process inventory (receive, pick, pack, ship) would be impaired. If the office area were to have a significant fire, computer systems, including the inventory management system, would be damaged or destroyed.

So, what are the critical business functions impacted by a fire in the warehouse? First, we have the sales function because inventory would be damaged. Second, we have the inventory function because physical systems for managing inventory would be damaged.

What are the processes impacted by a fire in the warehouse? The company has processes in place for the following:

1. Picking orders.
2. Packing orders.
3. Staging orders for shipment.
4. Tracking shipments.
5. Receiving new inventory.
6. Stocking new inventory.

7. Updating inventory systems with shipping and receiving data.
8. Managing damaged or missing inventory.
9. Processing returns of damaged or wrong items.
10. Inputting inventory data into inventory system.
11. Replenishing packing materials.
12. Repairing warehouse equipment.
13. Cleaning warehouse areas.

You can see from the list that items 11 through 13 are not critical processes. Other items on the list may not be mission-critical either, but we started with a full list of what goes on in the warehouse. If a fire engulfed the warehouse area, it's possible the building would be off-limits due to safety concerns, the offices might be filled with smoke and unusable, and the inventory might be smoke and water damaged by the fire suppression systems or by the water the fire department would hose in to put the fire out. Therefore, let's assume that a fire would impact all these processes listed. The company has no inventory it can ship to customers. What are the most important processes that have to get back up and running in order for the company to generate revenue and continue operations?

Remember, there are probably 14 other companies out there that are waiting for ABC Hardware to falter so they can swoop in and steal ABC's customers. ABC cannot afford to wait around for the water to dry and the smoke to clear before getting back into business. So, let's look at these first 10 items, along with criticality and comments, shown in Table 4.3.

Table 4.3 Example of Business Process and Criticality for Small Business

Business Process	Criticality	Comment
Picking orders	Mission-critical	Orders cannot be picked if inventory is damaged.
Packing orders	Mission-critical	Orders cannot be packed if they are not picked.
Staging orders for shipment	Mission-critical	Orders cannot be shipped if not picked and packed.
Tracking shipments	Mission-critical	Orders cannot be shipped if not picked and packed.
Receiving new inventory	Important	New inventory can be added to inventory system.
Stocking new inventory	Minor	New inventory cannot be stocked until damaged inventory is addressed.

Continued

Table 4.3 continued Example of Business Process and Criticality for Small Business

Business Process	Criticality	Comment
Updating inventory systems with ship/rec data	Mission-critical	No shipments going out but incoming inventory should be added so the company knows how much good inventory they have. Damaged inventory should be removed from stock as quickly as possible.
Managing damaged/ missing inventory	Mission-critical	Normally, managing damaged inventory is a minor process. In the aftermath of a fire, damaged inventory should be processed as quickly as possible to enable the company to dispose of it as quickly as possible.
Processing returns of damaged/wrong items from customers	Minor	Normally, processing damaged and returned items from customers would be a high priority. In the aftermath of a fire, this falls to a lower priority.
Inputting inventory data into inventory system	Mission-critical	In order for the company to sell its products, it needs to know, very quickly, what inventory it has that is sellable and what inventory it has that is damaged and must be discarded.

As you can see from this example, what normally might be high-priority processes shift to lower priorities in the aftermath of a fire. The key to recovery for this company is to sort out its inventory quickly so it knows what it can and cannot sell to customers. The IT systems are not damaged (though a few warehouse computers might need to be replaced) and order processing can still occur. This includes taking phone and online orders, processing orders, comparing orders to inventory levels, charging customer accounts or credit cards, and recording customer data (address, phone, etc.). Thus, the sales function for the company is relatively unharmed but the ability of the company to process and fulfill those sales is impacted.

The business impact analysis for this company now has identified the critical functions in the warehouse with regard to sales, inventory management, and shipping/receiving. The list is not exhaustive. For example, it does not include shipping supply replenishment. In the

immediate aftermath of the fire, shipments cannot go out so this isn't a problem. However, it's likely that shipping supplies have been destroyed either by fire, smoke, or water, and need to be replaced before any shipments can go out. If the entire warehouse is impacted, there may be no saleable inventory and shipments will have to wait. In other cases, there may still be saleable inventory and the lack of shipping supplies would actually become a major problem. Therefore, replenishing shipping supplies as a process in the aftermath of a disruption might be mission-critical. This is how walking through scenarios helps you see the mission-critical processes more clearly.

What is the maximum tolerable downtime for these critical business functions and processes? Some of this company's customers are custom homebuilders who are working on tight timelines. They will not wait for a delayed order from ABC Hardware and will look elsewhere for these products. Therefore, ABC believes that with most of their orders, they have one week to recover operations before they begin losing serious revenue. In the risk mitigation phase of their assessment, this company's staff can devise a number of strategies to deal with this scenario either to prevent a fire from occurring or to create alternate fulfillment strategies in the event a fire does occur.

You can continue to expand this example to include other data. For example, you can include the expected financial impact, as shown in Table 4.4. The example is not complete but just shows the beginning of this process as a sample of how you might capture financial impact data. The first function, the sales function, in this example, is not immediately impacted by the fire in the warehouse. Sales are still generated through the Web site and sales people may still be able to access CRM systems and other sales tools to generate sales. The problem is not on the sales generation side but the order fulfillment side. At some point, the company's inability to process inventory and orders will affect sales. Customers whose orders are delayed may cancel, rumors may cause other customers to order from your competitors. If you can't receive new inventory or ship out existing orders, these will eventually impact sales, but not immediately. If you can forecast the delayed financial impact, that's great, but if you can't, just make a note that there is one down the line. We've also included an increased cost for customer service. If you have a fire and word gets out, customers may call about their orders, call to change or cancel their orders, or call to get assurance their order is in process. This may generate more work for customer service, which may need to bring in temporary help to staff the phones or work overtime to handle the increased volume.

Table 4.4 Financial Impact Example

Business Function	Business Process	Financial Impact
Sales	Generating new orders	Delayed impact
Warehouse	Picking orders	$2,000 per day
	Packing orders	$2,000 per day
	Shipping orders	$10,000 per day
	Receiving inventory	$4,500 per day
Customer service	Handle customer problems	$3,000

So far, we've seen little or no IT impact. The damage was contained to the warehouse and other than three computers used at the shipping and receiving stations, there was no other impact to IT. However, there are other IT tie-ins. For example, how will the company know the exact status of the inventory? When was the last inventory count performed? What is the status of the orders that were picked and packed—were they shipped or not? Which customer orders went out and which were on the dock awaiting shipment? Which returns were on the dock when the fire started and which were already processed? In this case, the company needs to quickly figure out the current status of its inventory as well as the status of customer sales and returns. It needs to know exactly what the status of everything is so that it can figure out what to do and in what order. IT may need to run special reports, print out inventory, shipment, or order lists in order to help warehouse functions get up and running again. These are disaster recovery tasks that the warehouse and IT staff will have to work together on to determine what might be needed.

You can extend this scenario and ask, what if the IT systems were located next to the warehouse and they were destroyed by fire? What if the fire started in the server room and spread to the warehouse? Now the scenario has changed significantly because not only do you have damaged inventory and uncertain status of shipments but you don't have IT system data immediately available to help sort things out. Sales data, inventory status, payables, receivables are all unavailable. The server room is charred, all systems are unusable. Now what?

Let's extend this just a bit so you can get the bigger picture. Table 4.5 shows some of the other operational impacts that might occur as a result of a warehouse fire. The impact on operations shows, for example, that customer perception is not impacted in the sales function. Customers may or may not know about the warehouse fire and if they can still place their order via the phone or Web, there is no immediate impact to customer perception. The same holds true for the customer perception of picking and packing orders. Customers usually don't know how their order shows up at their door (nor do they usually care), they care that the right products show up on time. Therefore, we begin to see a customer perception

impact in the processes of "ship orders" and "receive inventory." If inventory can't be shipped, customers don't receive their orders as promised and this impacts customer perception. If inventory can't be received, it isn't available for sale and the customer sees that products are out of stock. We won't go through every cell in the grid, but you can use this to understand how various operations are impacted by a warehouse fire. The employee impact, in this case, is focused on warehouse staff, who are highly impacted by the warehouse fire. Though we did not do it in this example, you could also document the key knowledge and expertise needed to carry out these functions. For example, the key skills needed in this case are people who know how to manage inventory so that orders are properly filled and inventory levels are properly tracked. This data can be added, as appropriate. The same can be done for the IT side of the process. If IT systems were down, which processes would be impacted and how would other operations be impacted? What skills and expertise would be needed for workarounds and recovery?

Table 4.5 Operational Impact of Warehouse Fire

Business Function	Business Process	Cash Flow	Investor/ Market Confidence	Market Share	Competitive Position	Customer Perception	Employee Impact
Sales	Generate new orders	Medium	Medium	Medium	High	N/A	Low
Warehouse	Pick orders	High	Medium	Medium	High	N/A	High
	Pack orders	High	Medium	Medium	High	N/A	High
	Ship orders	High	Medium	High	High	High	High
	Receive inventory	Medium	N/A	N/A	N/A	High	High
Customer service	Handle customer problems	Low	Low	Low	Medium	High	High

As you can see, this scenario focused just on the warehouse department. The warehouse manager or someone designated by the manager should participate in this business continuity planning process. Only someone working in the warehouse is going to be familiar enough with the various day-to-day processes to generate a realistic view of the impact of various business disruptions. Once they have walked through all the risk scenarios (we mentioned fire, flood, chemical spill, and upstream/downstream impacts earlier), they can assign the criticality, the maximum tolerable downtime, the operational impact, financial impact, and the employee impact.

You may also choose to include additional columns in your impact table (or in your analysis if you choose not to use a tabular format) such as the financial impact and the legal impact. In this scenario, we also could have included the dependencies. Sales are impacted by the availability of inventory data (you can't sell inventory you don't have on hand or on

order). Receivables are impacted by the ability to pick, pack, and ship inventory. Payables are impacted by the ability to receive inventory and manage missing/damaged inventory. Payroll is impacted by having to work additional hours to manage inventory damage from the fire as well as to perform work outside the normal scope of warehouse operations. Expenses go up because additional supplies must be purchased to replace the supplies lost in the fire. Sales are down because shipments cannot go out until inventory is adjusted and some customers have purchased elsewhere. The building has to be cleaned by a professional company that specializes in recovering from fire damage and that impacts operations and increases the company's expenses with an unplanned expenditure.

What you'll discover from this process is that as you walk through these scenarios, you'll begin getting ideas about how to mitigate the impact of these disruptions. In Chapter 5, when we discuss mitigation strategies, you'll find that one mitigation strategy might be helpful for three or four different risk scenarios. Thus, what would reduce your risk in the event of a fire might also be an excellent strategy for mitigating the risk of flooding or a chemical spill in the area. These economies are found only by thoroughly assessing risks and impacts so you can see the big picture and develop optimal mitigation strategies.

Now that you have identified the critical business processes for the warehouse department, you can also look at the impact a flood would have. For example, if employees cannot get to work, if trucks cannot come in to deliver inventory, if trucks cannot pick up shipments, many of these activities are impacted. If the warehouse area is flooded, you have a similar problem as you did with a fire. If the area surrounding the building is flooded but your inventory and IT systems remain in tact, you have a different set of challenges.

By identifying the critical business functions and processes, you can clearly see the impact various risk sources would have on the business. You can assign criticality and maximum tolerable downtime in preparation for developing effective strategies for addressing these risks.

If you were to continue with this example, you would define specific recovery objectives based on criticality, you would identify organizational and system dependencies, and you would define work-around procedures that could be used. This would comprise the impact analysis for the warehouse department for the risk of fire. If you expand it to include the same assessments for each threat source identified in your risk assessment, you would have a comprehensive impact analysis for your warehouse department. Each department in the company would complete this process and you'd have the risk assessment and impact analysis for the entire company. As you can see from just this small example, it's a large undertaking and may well take more time than any other part of your project. Allow enough time to get this completed but don't let it get long and drawn out. Most of this can be completed by departments in a reasonable amount of time, though the more complex the business systems, the longer it will take to perform this assessment.

Preparing the Business Impact Analysis Report

There is no standardized format for a business impact analysis report and, as with many other processes, this document will likely follow your company's standard format. At minimum, the report should include the business functions, the criticality and impact assessments (see the list is Table 4.2) and the maximum tolerable downtime (MTD) assessment for each. Dependencies, both internal and external, should be noted and the correlation to IT systems should be delineated.

This report should be prepared in draft format with initial impact findings and issues to be resolved. The participating managers, SMEs, and BC/DR team members should review the findings. Revise the report based on participant's feedback to the draft document. If needed, you can schedule a review meeting to discuss the finding in the draft. Often this is helpful (and needed) to resolve conflicts with regard to the criticality and maximum tolerable downtime ratings, since there is a correlation between these ratings and the cost of mitigating the risks and reducing downtime. Once the feedback has been gathered, revise the draft and finalize the document. This document, depicted at the outset of this chapter in Figure 3.2, is used along with the risk assessment as an input to the risk mitigation process. To assist you in preparing your final report, we've recapped the elements you may choose to include.

- Key processes and functions
- Process and resource interdependence
- IT dependencies
- Criticality and impact on operations
- Backlog information
- Key roles, positions, skills, knowledge, expertise needed
- Recovery time requirements
- Recovery resources
- Service level agreements
- Technology (IT and non-IT technology)
- Financial, legal, operations, market, staff impacts
- Work-around procedures
- Remote work, workload shifting
- Business data, key records

- Reporting
- Competitive impact
- Investor/market impact
- Customer perception impact
- Other (business-specific data not already included)

Summary

Performing the business impact analysis requires you to look at your entire organization from top to bottom. You can begin by gathering subject matter experts, whether division heads, departmental managers, or designated staff, from various parts of your company. These people should be those in the company best able to answer the questions related to critical business activities. This relates to how your company generates revenues, tracks customers and sales, and other key business processes.

Data can be gathered using questionnaires, interview, workshops, documents, and research. There are pros and cons to each approach, so be sure to select the method most appropriate to your organization. Since each company is unique, there is no "one size fits all" template you can use to delineate all critical business processes for all companies. However, throughout this chapter, we discussed a wide variety of business functions, processes, and approaches that can help you develop a comprehensive list of your company's critical processes as well as the key roles, expertise, and knowledge needed to carry out those critical processes.

Once this data is collected, each process must be assessed for criticality. In the big picture, how critical is each business process to your company's ability to continue operating? Using a three- or four-point rating system will help you look across the depth and breadth of your organization to understand which processes and functions are mission-critical, which are vital or essential, which are important, and which are minor. Your risk mitigation planning efforts will focus first on mission-critical processes and then to vital or essential processes.

You'll also need to develop your recovery time objectives (RTO) for each critical function. In some cases, you might choose to associate a recovery time with criticality ratings. For example, mission-critical functions might need to be recovered within 24 hours whereas vital or essential functions might need to be recovered within 72 hours. Alternately, you can assign criticality and then assign recovery time objectives to each process individually. This might make more sense in companies where there are numerous mission-critical processes that cannot be simultaneously addressed. Again, this is a decision you and your team have to make regarding recovery objectives. Input from division or departmental experts is key to understanding required recovery timeframes as well as key interdependencies that exist among departments, processes, and systems.

There is a relationship between the cost of recovery and the cost of downtime. Each company has to assess these costs and make decisions regarding the optimal point of intersection. The longer the company goes without a key process, the more expensive it becomes due to loss of sales and increase in costs associated with the outage. However, recovery costs go down the longer you have to recover. If you need to recover within hours, your costs to provide this type of recovery capability will be significantly higher than if you need to recover within days. The point at which downtime costs and recovery costs intersect is the optimal point for planning, though in the real world, it can be difficult to determine the

exact point of intersection. Keeping this concept in mind, however, will help you find the best solutions for your company.

The business impact analysis uses business functions, business processes, and IT systems as the input points. The analysis is performed so that each process is identified and analyzed. The output for each process and function includes criticality assessment, financial impact analysis, operational impact analysis, recovery objectives, dependencies, and work-around procedures. When this is documented for each business function and key business process, you have a comprehensive look at your company and a solid business impact analysis.

Solutions Fast Track

Business Impact Analysis Overview

- ☑ After identifying risks and threats to the company, the business impact must be evaluated. Key business functions and processes are viewed in light of risk assessment data.
- ☑ The impact of disruptions not only to your business but to upstream and downstream partners needs to be considered.
- ☑ Consider the impact on corporate employees including physical or emotional injuries in the aftermath of a serious event or natural disaster. People respond in many ways to disasters and your plan must have the flexibility to allow for a variety of responses.
- ☑ For each key business process, critical objectives, timelines, dependencies, and impact must be understood and analyzed.
- ☑ The impact of the disruption of key business functions is assessed and prioritized so that risk mitigation strategies can be developed.

Understanding Impact Criticality

- ☑ Not all business functions and processes are mission-critical. Your risk mitigation strategy planning usually is limited to those functions and processes that are vital to the ongoing operations of the company.
- ☑ You can use a three- or four-point system of rating criticality. The four-point system ratings are mission-critical, vital (essential), important, minor. If a three-point system works better for you, you can use mission-critical, important, and minor. Define these clearly so they are used consistently across the organization.

- ☑ All processes should be assessed for criticality. Recovery objectives must also be assigned. Some companies assign the recovery time with the criticality. Therefore, mission-critical would have a recovery objective of 0–4 hours, for example. Other companies choose to set recovery objectives separately.
- ☑ The total time it takes to recover from a business disruption includes the recovery point objective, which is the lag between the time of the last good backup and the business disruption, the time it takes to recover systems, the time it takes to recover data, and the testing and verification of repaired systems. This is often called the maximum tolerable downtime (MTD) or maximum tolerable outage (MTO).
- ☑ There is an optimal point between the cost of downtime and the cost of recovery. The longer systems are down, the more expensive it is for your company. The shorter the required recovery time, the more expensive it is for your company. Therefore, the intersection of the cost of downtime and the cost of recovery is the optimal point. This is not always easy to determine but the concept helps in your planning efforts.

Identifying Business Functions

- ☑ Business functions are areas of the company that have specific roles or purposes such as sales, operations, finance, or HR. Business processes are the defined methods and actions used to achieve those purposes. Both functions and processes must be assessed in order to fully understand the company's critical work.
- ☑ The most common business functions include facilities, security, HR, IT, legal, compliance, manufacturing/assembly, marketing/sales, operations, research/development, and warehouse/inventory.
- ☑ The most common business processes include sales, invoicing, inventory management, and payroll, to name just a few.

Gathering Impact Data

- ☑ Gathering data for your business impact analysis is a significant undertaking. Enlisting subject matter experts (SME) from around the company is vital to your success.
- ☑ Using scenario-based questions, you can help SMEs understand what you're asking of them and help them envision potential problems. The more realistic your scenarios, the better data you'll gather.

- ☑ The data you gather should include the business function, process, criticality, time to recovery, dependencies, financial and operational impact, and other relevant data.
- ☑ You can use questionnaires, interviews, workshops, documents, and research to gather data. There are pros and cons to each approach; use the one that best fits your organization's way of doing business.

Determining Impact

- ☑ Determining the impact runs the gamut from financial to legal to operational to environmental and beyond. It's important to understand the impact to the company from these various perspectives, even if your focus is on the impact related to IT systems.
- ☑ The impact of a business disruption may have serious legal, financial, or regulatory consequences. These typically come from outside the organization and should be included in your planning. It's sometimes easy to miss these external elements when focusing solely on internal business impacts.
- ☑ The company's reputation in the community, region, or marketplace can be greatly impacted by a business disruption, especially if that disruption has to do with data security, data loss, or other sensitive areas. This should also be taken into consideration as you look at the impact analysis.

Business Impact Analysis Data Points

- ☑ There are numerous data points that can be collected about business processes across the organization. A comprehensive look will include these data points along with the interdependencies and impact on/with IT systems.
- ☑ For each critical business process, the impact to and impact from IT systems should be mapped out. In some cases, the disruption of a business process impacts IT systems. In other cases, the disruption of business processes does not impact IT but the disruption of IT systems, either primary or secondary, can impact key business processes. These interdependencies must be clearly understood and documented.
- ☑ External elements such as regulatory compliance, reporting, and corporate reputation must also be addressed. Again, the IT relationship must also be addressed. Often there is no leeway in meeting financial or legal obligations, regardless of the nature of the business disruption. There may be a bit of flexibility if a large natural disaster impacts the firm, but an isolated event such as localized flooding or fire will not alter regulatory, legal, or financial requirements on the firm.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: There seem to be far too many things to consider when doing the business impact analysis. I don't really know where to start. Any suggestions to make this process less overwhelming?

A: The business impact analysis is probably the largest data gathering aspect of this entire project and it can be overwhelming. The key to success is first to identify the various business functions then recruit experts from each function to participate. If you have to sit down and map all this out yourself, you not only will be overwhelmed, you'll also probably have lots of gaps and errors. This has to be an organizational effort, not just something the BC/DR team does off in a corner. Next, if you create a clear, concise set of questions that you want each subject matter expert to respond to, you have a much better chance of getting good data. In some companies, creating a series of workshops and working together in a less formal atmosphere may make this process a bit more interesting and productive. If you break it down by function or department and just start working your way through the data, you'll find you make it through this process a bit more easily. It's a big job but defining the segments and working systematically through it will help you get there successfully.

Q: I'm an IT analyst and a lot of this information doesn't relate to my job or role in the project. Can't I just skip over this section?

A: You could, but not if you want to have a successful project. Even if your role is limited to assessing IT functions, you need to understand how your company conducts business. Without that understanding, you won't be able to make intelligent assessments about IT systems. Sure, you know which servers are running which applications, you understand user access and security, but how does this relate to the day-to-day activities in your company? If the building were to burn to the ground with your IT systems in it, how would you prioritize your next steps? If you don't know which activities are mission-critical, you can't make intelligent assessments about which systems should be restored first. Certainly, there may be IT-related constraints with regard to the order or priority of system recovery, but you also need to consider the bigger picture. Critical business processes must resume first, regardless of where they fall in the IT world view. Therefore,

participating fully in this process will make you better able to participate fully on this team and it will also help you be a more productive contributor to the overall business.

Q: You didn't spend much time talking about IT systems in this chapter. I thought this book was focusing on business continuity and disaster recovery for IT professionals. Did I miss something?

A: No you didn't miss anything. Any IT professional needs to focus on these businesswide issues, regardless of whether you're heading up the BC/DR effort or just focusing on IT needs. We didn't spend an undue amount of time on IT systems at this juncture because this section focuses specifically on the *business* impact analysis. You should include your IT systems as part of your assessment, just as you included other functions such as warehouse or marketing. However, since you know your IT systems and your IT processes intimately, we focused instead on areas that are likely to be less familiar to you. The processes and procedures discussed in this chapter, however, should be applied to your IT functions and processes as well. The interdependency of IT systems with other business functions is important and that's why we focused on that area more than strictly on IT systems. We'll look at IT systems in more detail in upcoming chapters.