3

Conducting a Business Impact and Recoverability Analysis

The business impact analysis, or BIA, is probably the most important component of your entire disaster recovery project. This is the part of the project that defines and quantifies all the reasons why you are going through the trouble of producing a disaster recovery plan in the first place. The more factual, comprehensive, understandable, and informative your BIA is, the better your chances are for success in the disaster recovery planning project. If your BIA clearly communicates the inherent vulnerabilities of the System i5, iSeries, and other systems, you will win the endorsement, support, and funding of senior management. A BIA is a formal method of assessing risks and determining the potential economic loss that could occur as a result of these risks. Probably the most feared risk in IT, and the one viewed as most problematic by IT managers today, is the need to recover from a complete disruption of computing services . . . in other words, the loss of the data center or the loss of customer server data.

To support the criticality and associated financial burden of a critical system loss, all business functions must be identified and analyzed during a BIA project. Then, these business functions can be aligned with supporting IT infrastructure and ranked as either critical, essential, or desirable (nice to have). Each process is evaluated to determine the potential revenue loss that would be incurred in the event of any such disruption. The DR planning team should also expand the business impact analysis to review the legal and regulatory ramifications associated with no delivery of goods sold and the contractual requirements to determine the consequences of any prolonged business interruption. The result of the BIA will help design the DR planning roadmap by assisting the recovery team in developing procedures for recovering from various types of disasters. Recommendations will be identified during the BIA.

Management representing the business will need to understand the cost of not being able to use IT services. Jointly, the recovery team and management must anticipate capital spending requirements for any strategic solutions presented to mitigate some of the projected revenue loss. Typically, it makes sense to demonstrate a return on investment (ROI) when you identify specific technological solutions required to mitigate the risk and damage of a disaster.

A BIA is an information-gathering exercise designed to methodically identify:

- The business functions performed by an organization
- The resources (server applications) required to support each business function performed
- Interdependencies between business functions (the information flow)
- The impact(s) of not performing a specific business function
- The criticality of each process
- A Recovery Time Objective (RTO) for each business function
- A Recovery Point Objective (RPO) for the data that supports each business function

This process lays the foundation for selecting the required recovery strategy, recovery scope, and accepted timelines for disaster recovery. The benefits derived from performing such a comprehensive BIA include the following:

- Reduce legal liability.
- Minimize the potential revenue loss.
- Decrease exposures.
- Minimize the loss of data.
- Minimize the length of the outage.
- Reduce the probability of any disaster occurrence.
- Ensure an organized recovery of critical applications.
- Reduce the reliance on specific personnel.
- Ensure legal, statutory, and regulatory compliance.

Starting the Business Impact Analysis

The disaster recovery coordinator should be involved in the entire BIA process. The role of the DR coordinator is to manage the process, ensuring its effectiveness within the DR planning project. A time commitment and specific resources will be needed to develop the BIA. The following senior executives within your organization will need to participate:

- Chief financial officer
- Chief information officer
- Vice-president of operations
- Risk management officer
- Security officer
- Facilities manager
- Senior management from key business areas
- IT recovery team

The recovery team should define the scope of the analysis and be involved in setting priorities, reviewing the BIA findings, and making recommendations. From the DR planning team's perspective, the objective of a disaster recovery plan is to enhance the survivability of your organization in a disaster.

Tangible Costs

When information on the System i5 server is not available to users for any reason, you have downtime. Very often, this will cause the business to completely stop. When the business stops, it gets very expensive, very quickly! You must understand how important this analysis is to the survival of the company. Simply stated, information is the lifeblood of a company. It is crucial to know the server on which all critical information resides and the associated plan for its acceptable, timely recovery.

Calculating costs associated with downtime is much more difficult than it would first appear. Your business executives deal with everyday numbers associated with their specific line of business, and they can normally provide reasonably quick, reliable financial information. The total of all revenue information for all lines of business is considered the tangible cost of downtime. However, this is still a 50,000-foot view of the total impact, which makes it incomplete. There are other tangible and intangible costs to consider, as shown in Figure 3.1. These include lost revenue, brand reputation, the cost of wages for idled workers, interim (temporary) labor costs, lost inventory, marketing costs, bank fees, late penalties, SLA issues, lost customers, and legal costs.

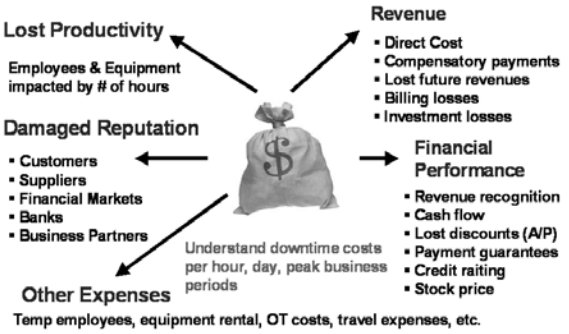

Figure 3.1: Many tangible and intangible costs are associated with downtime.

Lost Revenue

The most obvious tangible cost of downtime is lost revenue. We can all relate to this effect on the company's bottom line. If your organization cannot process customer orders, it cannot conduct business. With 24/7 electronic commerce, this problem is magnified. Sales depend entirely on system availability.

Having 24/7 availability implies the following:

- 24/7 customer support
- 24/7 services
- 24/7 e-commerce
- 24/7 manufacturing
- Expanded Internet dependence (email)
- Realtime enterprise strategy/business Service Level Agreements
- Global marketplace; mobile workforce

One way to estimate the revenue lost due to a downtime event is to look at normal hourly sales and then multiply that figure by the number of hours of

downtime. Be sure to consider peak selling periods, like the Christmas season in the retail industry. Some typical downtime costs are shown in Figure 3.2.

Average Cost per Hour of Downtime by Industry

Finance:	Brokerage Operations	$5.15 Million
Finance:	Credit Card Authorizations	$3.10 Million
Telecom		$2.00 Million
Manufacturing		$1.60 Million
Online Retail		$ 613,000
Communications:	Internet Provider	$ 90,000
Transportation		$ 89,500
Media:	Ticket Sales	$ 90,000
Transportation:	Package Shipping	$ 28,000

Source: The Meta Group & Contingency Planning Research

Figure 3.2: This will give you an idea of the impact of downtime in various industries.

Lost Productivity

Employees are not laid off when a major system is down for an hour or two. Some employees will be idle, but their salaries and wages will continue to be paid. Others might get sent home with full pay. Still others might be able to do some work, but their output will likely be of lesser value to the company's bottom line.

According to *Dunn & Bradstreet*, 59% of Fortune 500 companies experience a minimum of 1.7 hours of downtime a week. This includes all planned and unplanned outages. Assume a company has a total of 1,000 employees affected by this outage at an average hourly wage of $21. The downtime would cost the company $33,600 per week (1,000 x $21.00 x 1.6), or $1,747,200 per year. This, of course, excludes the cost of benefits. Companies are in business to make money. The value employees contribute is usually greater than the cost of employing them. Therefore, this method provides only a very conservative estimate of the labor cost of downtime.

An additional calculation is required for recovery labor. After a period of downtime, employees not only have to do their regular jobs of processing

current data, but they must also reenter any data that was lost or not entered during the system outage. This means additional hours of work, frequently on an overtime basis. Secondly, there could be overtime pay in the plant to catch up on the order processing. Overtime is expensive labor.

Late Fees and Penalties

Some companies like those in Just in Time (JIT) industries are subject to severe penalties for not delivering product on time. This is particularly true in the automotive industry. The "Big Three" do not care about your particular system woes. Their expectation is "Just get me the inventory so I can make cars." The fines can be very substantial, your vendor rating could drop, or your company could even get removed as a supplier.

In JIT industries, you might also be rated by the number of failed electronic documentation slips (Advance Shipping Notices) supporting trucking or rail deliveries. Therefore, even if you manage to get the product to your customer's doors, if your system cannot produce customer-required RFID or shipping documents, the product gets turned away. That is extremely costly.

Legal Costs

Depending on the nature of the affected systems, the legal costs associated with downtime can be significant. Downtime could cause a significant drop in share price. Shareholders might even initiate a class-action suit if they believe that management and the board were negligent in protecting vital assets, like the company's private data.

In addition, your partners can and will turn on you. If two companies form a business partnership in which one company's ability to conduct business depends on the availability of the other's computer systems, depending on the legal structure of the partnership, the second company might be liable for profits lost by the first during any significant downtime event.

Intangible Costs

Understanding the tangible costs is just the beginning. It is equally important in any downtime calculation to identify and quantify the intangible costs, which are not always clearly understood. These include the long-term impact of damaged reputations and future lost business from defecting customers, among others. These intangible costs are real.

For example, a perishable-goods producer like a meat supplier might have to dispose of spoiled inventory, or a manufacturer might incur setup costs to restart a stopped assembly line when inventory feeds a secondary finished-good line. I have had clients give away product because they could not get it on trucks to reach store shelves in an acceptable amount of time.

It is impossible to list all the potential intangible costs, as many are specific to the affected company and its particular environment. However, here are some typical ones:

- Lost business opportunities
- Loss of employees and/or employee morale
- Decrease in stock value
- Loss of customer/partner goodwill
- Brand damage
- Driving business to competitor
- Bad publicity/press

Lost Opportunity

When customers and prospects are prevented from dealing with one company because of a network outage, some will not try again later. Instead, they will purchase the product from the competition. It's the dreaded online buyers! They double-click, wait, double-click. No response? They go surfing the Web for another solution. A company therefore loses not just the immediate

purchase of a potential customer; it also loses all the purchases that potential customer would have made over the life of the business relationship. This can add up to millions when weighed against how many potential clients were turned away and how much they could have purchased from you over the next five or 10 years.

Remedial Expenses

Large companies spend millions of dollars building their brands and protecting their corporate images. Constant, repeated downtime will harm a company's image. The impact could be felt in consumer confidence, sales, share value, and reputation. If a major downtime event causes a loss in brand appeal and consumer confidence, an expensive corporate-image and marketing campaign might be necessary to repair the damage. What about replacing lost customers who will not return? Market share is everything, and it takes years to establish it, with lots of sales and marketing cost.

The impact to your company should be measured as operating impact, financial impact, and compliance both legal and regulatory. Your business might be forced to operate in a manual mode for a significant period of time following a major catastrophic computing failure. This will, of course, affect the efficiency of your business and have a downstream effect on profits.

Your business might experience serious financial losses as a result of the business interruption, and many of those losses might not be covered by insurance. If your financial systems are crippled by inaccessibility of information, your cash flow will suffer. If payroll systems are affected, employees might not even want to work!

Lost revenues, additional costs to recover, fines and penalties, lost good will, and delayed collection of funds will all add up in a disaster. Once you have determined the impact of an incident on a business function, you can determine the recommended recovery timeframe for the function.

Identifying Mission-Critical Functions

During the business impact analysis, the DR planning team needs to identify the critical functions within the business. These can be identified by listing all functions performed, determining the impact that an incident would have on a business function, and estimating the business loss for the duration of an outage. This process is often most effectively achieved by gathering information from key business leaders via questionnaires or interviews.

The mission-critical business functions include all information, processes, activities, equipment, and personnel needed to continue operations if information systems become unavailable. To determine the mission-critical functions of your organization, each department should consider all important functions performed within that department. Here are some questions to ask, to begin the process:

- If the system was not available, how could the department continue to function?
- What happens if the system is not available for more than a working day, or two, or three?
- Can your department resort to manual processes?
- What is the minimum amount of workstations you can function with?
- What procedures would be necessary to limit exposure during online systems downtime?
- What happens if the data is lost and the system is restored with data that is 24 hours old? Can data be re-created?
- What special forms and supplies are needed?
- Do you have any IT systems you use outside of the primary data center, such as bank-payment connection software or digital certificates on a local desktop?
- Is a particular time in the business cycle, such as month-end, more critical than others?
- What are your critical IT applications?

- » Application name?
- » Application priority?
- » Special requirements?
- » Maximum outage (hours, days)?

Viewing the BIA process in terms of the needs of your business clearly states its importance to the disaster recovery plan. What is the priority associated with software applications such as your ERP system, in terms of importance to the business? Be aware that these questions might not be easily answered and might spark considerable discussion and controversy.

Do not exclude secondary applications, such as EDI and email. You might be surprised to find these applications supporting significant portions of the business without any recovery procedures at all.

The Workshop Approach

Your choices for gathering information about mission-critical functions include one-on-one interviews, written questionnaires, workshops, or a combination of these approaches. The culture of your organization will determine the best way to obtain the desired information within acceptable timelines. I personally prefer a workshop to kick things off, with a questionnaire as a take away. (A sample questionnaire is available in appendix A.) While one-on-one interviews can be helpful, they generally lack business objectivity and are very time-consuming.

I recommend inviting a group of no more than 10 senior executives at a time to a "Business Impact Workshop." I prefer an interactive session, and trust me, I ensure it becomes interactive very quickly. I send out an initial agenda outlining the scope and purpose of the meeting. Then, I send a high-level questionnaire asking the participants to evaluate the following four statements:

1. All IT systems are down and will be out indefinitely. At which time (1 hour, 12 hours, 1 day, 2 days) are you completely unable to perform business functions?
2. The systems will be back on–line by the end of the day after being down for 12 hours. However, they will be returned to you with yesterday's data. How does this affect you ?
3. What services does IT provide your line of business?
4. What priority (immediate, critical, important, vital, or deferred) would you assign to each application you use?

The workshop typically runs 60 to 90 minutes. Your goal during that time is to educate the group on disaster recovery, business impact, business functions, and alternatives for system recovery. Emphasize the need to validate business functions supporting servers, applications, and the specific data requirements for those applications in all critical areas, as identified by the executives. Have someone provide support in the workshop for white boarding activities, taking notes, etc. (This could be the disaster recovery coordinator.) Consider electronically recording the meeting, if that is an acceptable practice in your company. It is important to engage all the senior management, as you will certainly discover many business functions that overlap, and the needs of one department might be greater than those of another. The combined organizational needs are what you are looking to define in the BIA.

The workshop produces the following results:

- Provides a collaborative and self-validating exercise
- Allows you to educate executives about disaster recovery
- Removes "analysis paralysis" because of combined initiatives
- Minimizes problems with anecdotal informational about impacts, as everyone is in the same room

The workshop decreases the concern from the executives that they are writing their business needs in stone, or that this is going on deaf ears. Inform them

that IT is developing a best response to disaster to support their business requirements. They are simply providing educated opinions about the criticality of their business functions and their IT system needs, and nothing more. During this meeting, you're gathering information about what server applications support those critical business functions.

Produce meeting minutes. They will go a long way toward the project's success. Summarize the findings of the meeting back to the executive team for review, to ensure they clearly reflect management's thoughts and business needs. Most executives claim that their part of the business is extremely vital to the short-term viability of the company. This might be true, but it can be overstated. This is a common issue with BIAs, as every business leader states their access to systems and user data is critical to the survival of the business. The question to ask is whether they can then quantify this with supporting data.

The Interview Approach

Some organizations might be better suited to an informal interview process supported by a questionnaire, instead of a workshop. A list of questions should be developed in advance that you can use to conduct each interview. This makes for an organized approach and will keep the interviews on track. You do not need a comprehensive set of questions to occupy the entire interview period. Instead, a basic set of open-ended questions will enable you to informally learn enough about a department's critical business functions and use of IT-related services. A common set of questions will also provide the necessary consistency between interviews and ensure that you have the same base level of information to later draw from.

Here are some sample questions to ask (see the business impact analysis questionnaire in appendix A for more detail):

- All IT systems are down and will be out indefinitely. At which time (1 hour, 12 hours, 1 day, 2 days) are you completely unable to perform business functions?

- The systems will be back by the end of the day after being down for 12 hours. However, they will be returned to you with yesterday's data. How does this affect you ?
- What services does IT provide your line of business?
- What priority (immediate, critical, important, vital, or deferred) would you assign to each application you use?
- What does your business area do for the company?
- What services does IT provide your line of business?
- What systems and software do you need to run your department?
- What would happen if these systems were not available to you?
- Do you have any manual work-arounds?
- What would you do if you had no access to IT systems for *x* hours or *y* days?
- At what time do you send staff home during an outage? How many do you send?

It is important to take extensive notes. You will need to know exactly who said what at a later date. Encourage interviewees to respond in terms of direct impact, future impact, lost revenue over different time periods, amounts of services needed for a variety of disaster scenarios, staff impact, SLAs, penalties, etc.

Outage Impact

Once the mission-critical functions have been documented, it is important to determine the financial impact of an outage to these functions. Consider the impact in a complete computer loss and an outage that is 24 hours long with loss of customer data. Other considerations might include the timing of the disaster, such as the potential impact of a disaster at the end of the busiest sales month.

When analyzing critical systems, consider the following:

- Systems relied on to perform critical business functions, their interfaces, and their maximum acceptable outage time
- Dependencies between business functions
- Dependencies between departments
- Dependencies between systems
- Dependencies between applications

Answers to the following should also be carefully analyzed:

- How much revenue would your company lose if its systems were unable to accept orders? (Multiply the average hourly revenue by the number of hours needed to recover.)
- What is the cost of lost productivity? (Add the payroll, taxes, benefits, and overtime for recovery and multiply by the number of all employees from all the affected business units.)
- What is the value of IT employee productivity lost while trying to resolve the problem?
- How much inventory will be lost or spoiled?
- What fines, fees, and/or compensatory payments will you have to pay? (Consider breach of contract, regulatory fines, and late-shipment or late-payment fees.)
- What sales and marketing efforts will you have to initiate to recover revenues, lost customer loyalty, reputation, and/or goodwill?
- What is the impact of not processing in each of the following areas:
  - » Customer service
  - » Noncompliance with government regulations
  - » Noncompliance with existing contracts
  - » Increase in personnel requirements
  - » Increased operating costs
  - » Loss of financial management capability

» Loss of competitive edge
» Loss of goodwill
» Negative media coverage
» Loss of stockholder confidence

IT to Verify Business Data

One of IT's objectives during a BIA is to understand how every piece of software relates to every business unit and how it all relates to every server. The next step in the process is to speak with the System i5 or iSeries/400 administrators and other IT staff, again preferably in a collaborative workshop instead of one-on-ones. This is to confirm what was communicated by the executive team to determine the following:

- Where does the application reside—data center and server name?
- How quickly could the application realistically be recovered today?
- Based on historical information, how many help desk calls are received?
- What priority would IT put on a particular application?
- Does this align with what the business said?

Once all of these lists are created for each business unit, it will become self-evident which applications, vendors, etc. are most critical. Determining what constitutes a mission-critical business unit will also affect your final product. Spreadsheets on business priority and application recovery objectives are used long-term as a part of your overall backup and recovery plan program.

Business Impact from Planned and Unplanned Outages

A complete BIA for IT identifies all the financial costs that affect your organization resulting from a system outage, whether planned or unplanned. Normally, the impact on your business is discussed only in the context of

unplanned outages. Unplanned downtime is any unscheduled event from scenarios such as natural disasters, power loss, network connectivity failures, and hardware failures. Since these events cause great financial hardship to an organization, they are, of course, highly visible.

While the BIA tends to measure only unplanned downtime and its associated costs, system downtime can be both planned and unplanned, as shown in Figure 3.3. Do not limit the scope of your business impact analysis. Consider that the majority of System i5 outages that affect your ability to perform business functions are planned. Planned downtime occurs when you have a scheduled interruption of services. In other words, you get a blessing or approval from the business to take the System i5 services down to do required work. Here are some planned downtime examples:

- Backup window—incremental, daily, and full system
- IBM and third-party software upgrades
- IBM and third-party PTFs/Service Packs
- Application maintenance
- Database file maintenance (reorgs)
- Hardware upgrades

Identify all these outages and calculate the total hours in a year that are set aside for them. Examine the daily backup window, system or ERP application maintenance, or other related support needs for your organization. You will find these numbers for a year quite staggering. It's probably safe to say that you're already on a course to eliminate all planned downtime due to fundamental changes in your company's IT delivery model to the business. Use a thought process of identifying the cost for planned outages as a means of estimating the payback for an iSeries or System i5 high-availability solution. The most basic requirement for all high-availability solutions should start with the premise of eliminating planned downtime first, and then examine unplanned scenarios.

	Per Week	Per Year
Full Backups Weekly	3 hrs	156 hrs
Daily Backups	6 hrs	312 hrs
Software Installs		20 hrs
+ Housekeeping		24 hrs
= Planned Outages		512 hrs or 21.33 days/year

Figure 3.3: The planned downtime scorecard.

Ideally, you should discover and aim for the financial payback gained by eliminating all planned downtime to cover the cost for a solution to address unplanned downtime. Eliminating planned downtime can provide immediate payback to your business users, and it is easily measurable.

You already know exactly what constitutes all of the planned outages in your IT shop today. Eliminating planned downtime is immediate and measurable, but assigning a cost to an unplanned event that might never happen isn't so easy. Beyond lost revenues and productivity, the devastation caused by a critical application's loss for an extended time period might be so severe that it could permanently hurt your business. You must focus on worst-case scenarios because they go beyond the levels of acceptable business loss.

> 93% of all companies that experience significant data loss are out of business within five years.
>
> *Gartner Group, Inc.*

Recovery Time Objective vs. Recovery Point Objective

The BIA identifies all of the critical business functions and their supporting IT components. This is required to determine the Recovery Time Objective

(RTO) and Recovery Point Objective (RPO). The RTO is how soon the business units need to have their required services (IT applications) up and running. The RPO is the most recent point in time to which systems can be restored back. The shorter the RTO and RPO, the more complex, leading-edge, business resilient, and of course expensive the recovery solution becomes.

Not that long ago, most companies were open for business eight hours per day, Monday to Friday. Having the old AS/400 unavailable did not prevent any customer sales from occurring, because these transactions were usually conducted in person or over the phone, perhaps even recorded on carbon-copy paper. All of the transactions' details were gathered up through the day, and entered overnight. If some form of disaster shut down the AS/400 and the rest of computing services for a few days, the organization just continued working manually. The paper simply piled up, and when the systems came back online, the transactions would be entered. In other words, it was business as usual during an IT outage.

Today, you are faced with new realities. Employees, customers, and your suppliers are all interrelated . . . a global economy where the use of the Internet mandates a 24/7 business model. There is no official start or end to the business day. You are open 24 hours a day, every day. Systems are no longer isolated. They all interact with other systems to complete transactions, regardless of the hardware platform. The realities of today's business underscore the importance of delivering computing services and protecting the data that is your greatest corporate asset.

The goal for companies with no business tolerance for downtime is to achieve a state of readiness, where all critical systems and networks are continuously available, no matter what happens. Disaster recovery is a combination of how long you wait to bring your business back up after a failure (the RTO), and how much data the company is willing to lose due to a failure (the RPO). Finally, how much system availability your business is willing to pay for leads to the ROI. The interrelationship among RPO, RTO, and ROI is shown in Figure 3.4.

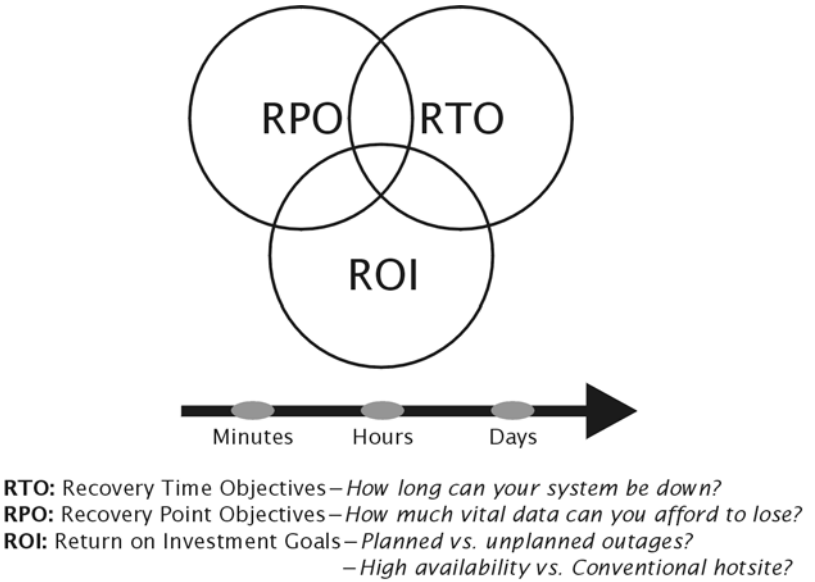

Figure 3.4: RPO, RTO, and ROI are intertwined in a business impact analysis.

The tolerance for RTO and RTP varies from industry to industry. Financial institutions, for example, require services back online in minutes, rather than hours. Even more critically, healthcare providers require emergency response immediately. Other industries can afford to be down 24 hours without access to IT. Organizations that cannot afford to lose more than a single minute's worth of transactional data must have strategies that include clustering or high availability, where online data is captured realtime in both the production and backup environments. Other organizations might find that tape backup programs supply ample data protection.

Recovery Time Objective (RTO)

As shown in Figure 3.5, the Recovery Time Objective (RTO) is the length of time required to recover from an unplanned outage as a result of a disaster. It includes the time required to resume normal operations for a specific application

server or set of applications servers. The RTO is directly related to the BIA and is normally stated as a specific time value in minutes, hours, or days.

Time is of the essence when recovering your company's lost data. While the IT folks are busy recovering your company data, your customers may be contacting other suppliers. Just in Time manufacturing, distribution, and electronic commerce have put a premium on systems availability and access to corporate data.

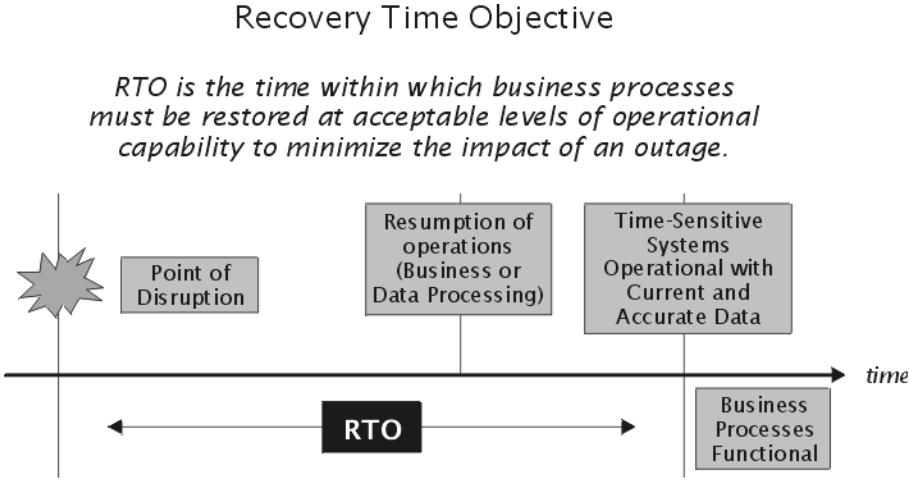

Figure 3.5: RTO is the length of time required to recover from a disaster.

The RTO is the acceptable time to recover all applications used in the business process, including recovery of applications, data, and end-user access to those applications within the maximum allowable downtime acceptable by the business. How long can your computer systems be made unavailable to support key business process? How long can you afford to be offline to your customers? Every business is unique, so the metrics for defining the RTO is different for each organization. You cannot answer these questions alone within the walls of IT. You must include the business directly, as they understand their business thresholds and service-level commitments to their customers.

To be cautious and save face, many organizations reactively set a 48-hour RTO as a place to start when defining initial DR recovery objectives, as shown in Figure 3.6. Aim for the quickest recovery your business can afford. When a disaster strikes your company, your competitors will jump at the chance to fill the void. An effective DR plan will ensure that you meet your RTO objectives. On the other hand, do not start with a 24-hour RTO without careful analysis. Twenty-four hours is not a lot of time to rebuild an entire server infrastructure.

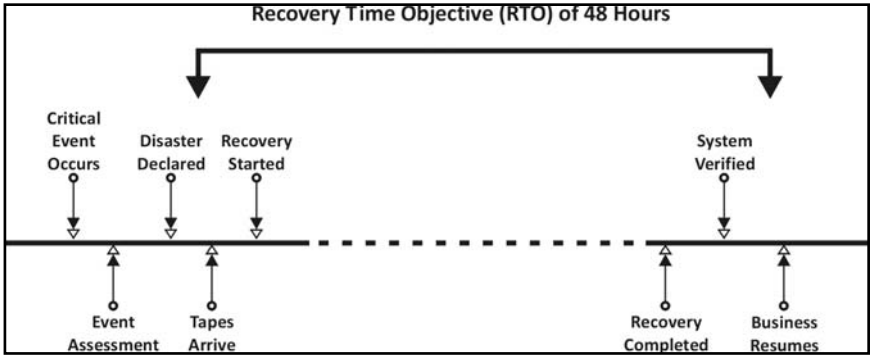

Figure 3.6: Many organizations typically start with a 48-hour RTO.

The system-restoration recovery timeline is the total length of time required to resume normal operations and application access after an unplanned outage occurs. The length of the recovery time depends on many factors. Table 3.1 walks through an example of typical recovery tasks in an outage. The total number of hours spent on these specific tasks will help determine the current capability to resume computing services after a system failure. This example is a single, stand-alone system with no LPAR considerations and includes 1.2 terabytes (TB) of disk utilizing a LTO3 tape drive.

Table 3.1: The Timeline to Rebuild a Sample System from Tape	
Recovery Tasks	**Time to Complete Task in hours**
Assess the disaster situation.	3 hours
Declare a disaster.	2 hours
Retrieve tapes from the offsite supplier.	1 howur
Transport key staff and backup tapes to the recovery site.	2 hours (Consider location of hotsite.)
Build the disk configuration.	4 hours
Restore LIC.	30 minutes
Restore OS/400 .	1.5 hours
Restore IBM programs.	30 minutes
Restore user data.	9 hours
Rebuild the IFS.	2 hours
Apply incremental data.	2 hours
Rebuild security.	30 minutes
Configure and redirect networks.	1 hour
Perform IPL.	30 minutes
Test and validate.	1 hour
Total Time	**30.5 hours**

With recovery at commercial hotsites, typically located out of state, you must plan for additional time to support the extended travel requirements. This typically will include airline travel to your destination. In accounting for travel arrangements for critical staff, do not assume everyone designated to travel has the personal funds to secure an airline ticket. Last-minute air travel can be really expensive.

Once you have determined how long your business can afford to be down, your RTO objectives will become obvious and accepted by the business. You will have to implement technological solutions to both manage the business expectations for downtime and observe your financial budget constraints. The shorter your RTO, the higher your financial investment will be towards an iSeries high availability, or System i5 clustering solution. Additional

considerations would be required for site redundancy, as well. You will need to put the systems in another location to support your reduced RTO solution. It is very possible that you simply cannot afford the expenditure to meet your business RTO. In these situations, the business will have to accept the risk associated with a lesser IT deliverable.

Recovery Point Objective (RPO)

The point in time to which server data must be restored to resume back-to-normal processing of transactions without adversely affecting the organization is the Recovery Point Objective (RPO). Following any unplanned outage where data has been lost, you must ask yourself, "To what recovery point can I restore based on the most recent saved data?" How much data is actually lost, versus how much can your organization afford to lose? Never assume that, even if you can go back to last night's backup tapes, those backup tapes contain everything required to rebuild your iSeries/400 as of 24 hours ago.

Before you implement any type of backup solution, you need to consider what the impact of a system failure (complete loss of data) has on your business. In a situation where your iSeries/400 server has experienced some form of hardware or disk protection failure, you need to ask yourself "How re-creatable is the user data?" Keep in mind that most data transactions today are electronic and originate from many access points. What is the cost of lost data or missing transactions in your company? With a traditional tape backup strategy, every business transaction executed within the current day will be lost. For example, if your last backup finished at 2 a.m., and you had a disaster at 5 p.m. that same day, could you re-create the data entered during the business day? This implies you could lose from zero to 24 hours of business transactions. In a true 24/7 business model, that can be very significant.

Be careful about promising and delivering a 24-hour RPO. Careful consideration must be given for weekend activities, as shown in Figure 3.7. Many

IT departments are satisfied with this approach and have thus conceded the fact that 24 hours of data loss is completely acceptable to the organization for Monday to Friday processing. However, by including weekend business activities, the RPO exposure is increased three-fold over weekends. Ensure that this is agreeable at the executive level, as well as within your IT department!

The most important thing to consider in this definition is that RPO is the point in time where the recovery processing will return all your end users from the perspective of both the data and application processing. Loss of data can cost your company big money, or even close your business altogether. An increasingly common way to compare resiliency with server technologies is to look at the way each hardware technology handles resiliency. The RPO is the total acceptable data transaction loss when recovering from a disaster or system failure. IT shops that require an RPO of less then 24 hours or immediate recovery to the last completed transaction and its committed data require a much more data-resilient solution that would include one or several iSeries/400 solutions.

Figure 3.7: RPO exposure.

Recovery point is the exact point in time you'll be returned to after all your recovery processing activities have been completed successfully. This is the point from which you'll resume normal business operations. A recovery point will differ with each recovery solution employed. For shared/switched devices (IASP, Integrated Auxiliary Storage Pools), the recovery point is always what was last written to disk. Transaction changes still resident in memory that haven't been written to disk will simply be lost. This means that it's vital to use journaling with these solutions, to help ensure that changes to critical data are captured on disk as they occur.

For high availability, the recovery point is always what was last transmitted and received by the backup iSeries server. Any changes that haven't been completely transmitted, and in some way acknowledged, will be lost. Another factor to consider is the total line capacity. Insufficient bandwidth can cause latency and a backlog of transactions on the source system. Too often the line between the target and source system is not dedicated; it is shared with the Internet solution (company wide!).

The use of object journaling with synchronous replication for logical copies can help ensure that changes to critical data are transmitted as they occur. However, this requires lots of bandwidth. Typical installations utilize asynchronous replication and forgo the system acknowledgement.

The 24-Hour RPO

What does a typical tape backup and recovery solution deliver? The solution delivers a minimum of minutes to a maximum of 24 hours of lost business transactions. The reason for this gap is that in every tape backup solution, the backup usually occurs only once per day. This means that the combined time that includes exposure to data loss and efforts to rebuild is always measured in days. Yikes!

In the example in Figure 3.8, the System i5 server goes down with an SRC indicator light at 5 p.m. on Tuesday afternoon. This is not a site loss, just a server failure only. Subject to IBM hardware availability and response to the Severity 1 call, the server will be repaired sometime late Tuesday evening or early Wednesday. The restoration process will immediately follow, and late in the day Wednesday, the user data will be as it was on Monday night's 2 a.m. backup. All of Tuesday's data is lost. If there were further issues with the full backup tape media, the data loss and restore effort would reach back through the entire previous week.

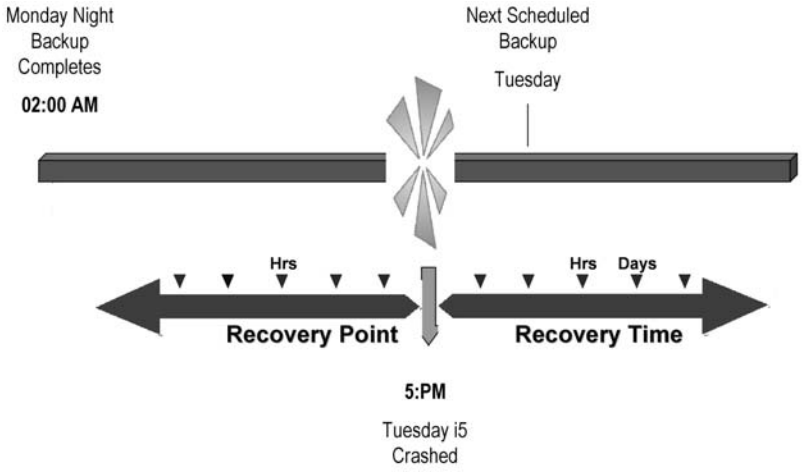

Figure 3.8: The real result of a 24-hour RPO.

Real-World Example: An Unacceptable 24-Hour RPO

I had a client that experienced a disaster in which the system was unavailable due to a multiple disk failure in their System i5. This meant a complete loss of data. The hardware repair effort took numerous attempts by the IBM hardware engineers, as the combination of failing disks, IOPs, IOA, and at the end the Raid card made it terribly difficult to troubleshoot. Many hours were lost in the hardware problem resolution. Then it was time to spend the 26 straight hours performing all recovery steps. Between formatting disk drives, restoring the key elements of the operating system, and recovering all user data from both weekly and daily tapes, the effort was fairly significant. Two terabytes significant! The total downtime was 36 hours.

The business was under great duress to ship all the product out. It had commitments to customers. The company had six warehouses scattered geographically within the continental U.S. Each was fully automated, with no means to operate manually. Union staff was sent home during the outage . . . very costly. The data that was restored on the system following the failure was more than 24 hours old. The inventory and warehouse systems

were as of a couple of days ago, including the day lost in bringing back the iSeries/400.

The arguments started between IT and business executives.

"How can we ship product out of our warehouses?," asked the VP of Logistics. "The information is totally unreliable. The system is feeding us product locations in the warehouse that do not contain the actual product. Has the product already shipped? Is the product sitting somewhere else in the warehouse on a pallet? Has the product been moved, or has the order been canceled altogether? Did we invoice already, were we about to, or do we invoice again to be safe?"

The situation was far worse than could have been imagined. The only course of action was to do a complete warehouse inventory position count and update the iSeries/400 with the quantities and locations on hand. This took 18 additional hours to complete, with lots of additional labor costs. The business had no choice; they could not operate with day-old information, as restored. The System i5 functionality was all intact, but the data told each user a different story. The aftermath was not pretty, as you can imagine. Nobody felt well enough informed from the business side as to what exactly IT was supposed to deliver. Secondly, nobody ever agreed to a 24-hour RPO of system data. This was simply unacceptable.

Do your business executives understand that everything your business sold, manufactured, serviced, etc. today will be lost if not captured by the nightly backup? I can assure you that many executives do not. This is a bad assumption many companies and IT make. Talk to your business executives, and ensure they are fully aware of what IT can deliver. An important lesson will be learned by all.

Every backup strategy must be examined closely to ensure both system and data are indeed recoverable. Many backup program designs are implemented and forgotten over time. An effective recovery strategy must always be designed first, followed by a backup strategy implementation. Typically, we perform this critical implementation task the other way. Usually, we are asked to recover from what we are given from last night's backup tapes, and then

try to bridge both the system and user data gaps. In other words, we perform reverse engineering.

Ensure your RPO is examined from both a mid-week and weekend failure, as this will most certainly present different models. Can you bring back everything on a Wednesday system loss as you could from a weekend failure?

Shifting Focus for Return on Investment (ROI)

The shift from the emphasis on data recoverability to continuous application availability is natural and logical. Your investment must support both planned and unplanned outages. It is important to understand that data resiliency itself doesn't provide a high-availability solution. It will simply help ensure that the data is available in the event of an outage. The movement in IT to shift from recovery of data from tape with a 24- to 48-hour systems recoverability solution to high availability is strategic and logical. The traditional approach for deploying high availability has been to replicate data from one system to another, with the primary objective being data recoverability only—in other words, disaster recovery.

The goal for the high-availability solution has evolved toward eliminating or minimizing planned outage events that require the production System i5 to be made unavailable to the business. Now during any such planned outage, the IT staff switches the end users to the backup or target server after carefully quiescing the primary system. After ensuring that all of the data on the primary and backup servers is identical, meaning no latency in sending or applying journal transactions, production applications are started on the target server.

Unplanned events account for 10% of all System i5 downtime. Unscheduled or unplanned downtime can be due to the following:

- Power outage
- Human error or program failure
- Unprotected disk or multiple-disk failure
- Other hardware failure

Planned events account for 90% of downtime. This downtime is due to the following:

- Daily/weekly/monthly saves
- Software installation/upgrade (OS, application, or middleware)
- PTF installs
- Operating systems upgrades
- Hardware upgrades

The decision with ROI is whether to purchase and implement a solution based on a 10% ROI, or aim for 100%.

Return on investment is the critical measure in any investment decision. The expected benefits of the recovery solution under consideration must exceed that project's anticipated costs to justify the inherent risks. The BIA tends to measure all unplanned downtime and its costs. We focus on this because, as stated earlier in this chapter, it goes beyond the level of acceptable. The devastation caused by a critical application's loss for an extended time period might be so severe that it mortally wounds your business. However, eliminating planned downtime can be immediate and measurable. Ideally, you should discover and aim for payback gained by eliminating planned downtime that covers the cost for a solution that inherently addresses unplanned downtime.

The Process of the BIA

There are six main steps to conducting the business impact analysis.

1. Set the Objectives of the Business Impact Analysis

The basic objective of the BIA questionnaire is the collection and evaluation of specific business functional and process information from the business.

Identify:

- The most critical business units
- All business processes and their priorities
- The business impacts of an extended interruption
- The maximum length of the outage a business unit can sustain before it has a significant negative operational impact on the company
- The key computing systems used by the business unit and the impact of no access to these systems
- The critical IT applications used by the business unit
- Any recovery complexity of the business unit's critical processes
- The recovery time requirements of the critical business unit
- The recovery point requirements for the critical business unit
- The recovery strategy and priorities of the business unit's critical processes

2. Determine Critical IT Applications

The responses should identify the most critical applications that are required by the business units to keep the business functioning. During the definition of recovery strategies, IT will have the opportunity to implement supporting protective measures and recovery strategies to ensure that the business unit's critical applications will be available in a timely and cost-effective manner during an actual recovery effort.

3. Distribute the BIA Questionnaire

Each of the business units will be required to complete an electronic BIA questionnaire. Supply the date by which the completed questionnaires should be returned to you. (A sample BIA questionnaire is available in the appendix.)

4. Receive and Validate the BIA Responses

The responses to the BIA questionnaires provide IT with information that will influence the recovery strategy and disaster recovery plan. It is, therefore, extremely important that you do the following:

- Make sure you receive a completed BIA questionnaire from every participating business unit.
- Ensure that each BIA questionnaire is fully completed and that the responses make sense.
- Store and maintain the questionnaires in an electronic file for audit purposes.
- Use the responses during the recovery strategy and plan-development phases.

Check each questionnaire for completeness and validity:

- Review each questionnaire and make sure that each question has been answered.
- Make sure that each answer is complete (not just a yes/no answer)
- Do not be afraid to send the questions back to the participant.

5. Consolidate the Responses

When all of the questionnaires have been returned, all of the questions have been answered completely, and the answers make sense, it is time to consolidate the responses and prepare a summary of the critical IT applications. This should be prepared using the "Mission-Critical IT Applications Worksheet" in Table 3.2. Start building this applications summary by listing all of the business units that submitted valid BIA questionnaires. For each business unit, include the business unit name. Next, for each business unit entry, include the following information in the appropriate columns:

- Application name
- Application priority
- Maximum outage (days)

Table 3.2: Mission-Critical Applications Worksheet

Date:		Company Name:		
Location	**Application Name**	**Application Priority**	**Maximum Outage (Days/Hours)**	**Maximum Data Loss (Days/Hours)**

These applications will be included in the final BIA presentation and report. The site's IT organization will be able to gain an early understanding of the critical business units' application requirements:

- The business unit's operational priority
- The business impacts of an extended interruption to the business unit's processes
- The maximum length of the outage a business unit can sustain before it has a significant negative operational impact on the company
- The vulnerability and recovery complexity of the business unit's critical processes
- The recovery timeframe requirements of the business unit
- The business unit's recovery strategy and plan development priorities

This information will be used in all of the early phases of the DR initiative. Review the findings to gain a business needs understanding of two key elements:

- The Recovery Time Objective (RTO) that defines the period of time in which a business unit must be able to resume its critical processes
- The Recovery Point Objective (RPO) that defines how much data the business can afford to lose

The business and the executive sponsor must agree with these RTOs and RPOs to help ensure the success of the BIA initiative.

6. Review the BIA Findings

You should now prepare a presentation of the BIA results for the executive sponsor and the participating business units' executives. Your basic goal is to get concurrence that the BIA results make sense and that there is a consensus agreement to proceed with the next phase of the disaster recovery planning project. Handouts of the presentation should be provided to all attendees.

Your presentation should cover the following:

- BIA phase summary
- Objectives
- BIA findings
- Prioritized critical business units by RTO and RPO
- Strategy/plan development schedules by RTO category
- Critical IT applications and potential issues
  - » Include a copy of the "Critical IT Application Worksheet" with an explanation of the contents.
- Vital assets and potential issues
- BIA phase action items

    - » Request approval of BIA findings from the business.
    - » Request approval to proceed with the next phase of the BCP initiative.
- Recovery strategy development phase
    - » Objectives
    - » Calendar timeframes
    - » Roles and responsibilities

During this presentation, you need to get the business units and the executive sponsor to agree with the following:

- The prioritized list of critical business units and their RTOs
- The proposed recovery strategy and plan development dates
- Vital assets issues
- Other recommended action items
- Your request to proceed to the recovery strategy

Obtain a consensus of approvals from the executive sponsor and the business unit owners.

Summary

Performing a BIA will provide your organization with a complete, holistic view of how your company uses IT services to conduct its business. Critical application server definition and disaster recovery capabilities will identify the tangible and intangible revenue impacts on the business. The BIA will clearly state the inherent vulnerabilities that face your organization, their quantifiable impact, and the acceptance of an agreed-upon solution. IT alone cannot make recovery decisions. The BIA provides IT a recovery roadmap aligned with the business's needs and deliverables.