

**Developing
a
Disaster Recovery/
Business Continuity
Plan**

Table of Contents

1. Abstract.....	1
2. Definitions	1
3. Plan basics.....	1
4. Build Senior Management Support.....	1
5. Conduct BIA	1
Business functions	2
Business related codes	2
Risks	2
Risk impact	2
Handling the risk.....	3
6. Determine Business Recovery Strategies.....	4
Value to the business	4
Relationship to other business functions.....	4
7. Prepare and implement the plan.....	4
Developing scenarios for most-likely events	4
Predictable events	4
Unpredictable events.....	5
Knowing what to protect	5
Recovery teams.....	5
Creating the team.....	5
Identifying team members	6
Team assignments.....	6
Notification options and procedures	6
Notification options	6
Notification procedures.....	6
Declaring a disaster.....	6
Who can declare	6
Response options	7
Handle locally	7
Handle remotely with contracted personnel (shared resources).....	7
Handle remotely with relocated personnel.....	7
Handle remotely with contract, own personnel.....	7
Hot sites, stand-by, cold sites.....	7
Recovering the business	8
Accessing the damage.....	8
Repairing the damage	8
Repair or restore	8
Replace	8
Relocate	8
Recovery declaration	9
External advisors	9
Writing the plan	9
8. Testing the plan	9
9. Maintaining the plan	9
10. Summary.....	10
Bibliography	

1. Abstract

This paper outlines the **general** requirements and techniques required to develop a disaster recovery/business continuity plan. These requirements apply to both government/non-profit and commercial organizations.

2. Definitions

A “disaster” for the purposes of this exercise, is “any condition that prevents an organization from carrying out its primary function(s).”

“Primary functions” are business functions that are the reason the entity exists. For a government agency, this normally is to provide for the safety and well-being of its constituency. For a non-profit organization, it is providing the service(s) specified in its mandate. For a business, the primary functions are producing a product or service to generate a profit.

3. Plan basics

Disaster recovery/business continuity plans typically include seven primary steps.ⁱ

1. Build senior management support and define recovery goals, objectives, and assumptions
2. Conduct a business impact analysis (BIA) of functional requirements
3. Determine business recovery strategies
4. Prepare and implement the plan
5. Perform realistic testing
6. Account for updating and refining the plan regularly
7. Prepare to declare a disaster



4. Build Senior Management Support

This is the **most critical** of all the steps. Lacking top-down support, the best plan is almost certain to fail. Indeed, a recent DMR Consulting Group Inc.ⁱⁱ DR/BC project encountered problems in the information gathering (BIA/risk analysis) stages due to lack of communicated commitment on the part of senior managers.



The Federal Emergency Management Agency (FEMA) states that “To be successful, emergency management requires upper management support. The chief executive sets the tone by authorizing planning to take place and directing senior management to get involved.”ⁱⁱⁱ



FEMA continues that the chief executive or plant manager should issue a mission statement to demonstrate the company’s commitment to emergency management. The statement should, according to FEMA^{iv},

- define the purpose of the plan and indicate that it will involve the entire organization
- define the authority and structure of the planning group.



Plans, in order to generate top-to-bottom support and to be effective, should be simple. According to the BMS Catastrophe, Inc.^v, “There are thousands of good words that can be written to ‘dress up’ your disaster plan, but a simple plan with the primary goals and priorities clearly stated will be much easier to successfully accomplish. Use the K.I.S.S. principle!”



5. Conduct BIA

The Business Impact Analysis (BIA) is used to identify

- business functions

- business-related federal, state, and local codes (covering such areas as personnel health and safety, environment, fire, transportation, zoning) and corporate policies and procedures^{vi}
- risks to the business functions such as^{vii}



civil disorder communications failure earthquake

electric failure fire flood



hazardous materials hurricane lightning

loss of key personnel sabotage tornado

vendors “other”

- impact of each risk
- means to avoid or mitigate the risks, or a decision to absorb the risk (allow to happen)

Business functions

Business functions refers first to “primary functions” as defined in [Definitions](#). Once the primary functions are identified, related functions are identified. Related functions can directly or indirectly place primary functions at risk.

Business related codes

Business-related codes impact both the business operation and the recovery process in the event of certain disaster conditions. Zoning laws, for example, may preclude rebuilding a facility on the present location. The DR/BC plan must be aware of codes that could impact the recovery operation.

In addition to state and municipal codes, plans also should be aware of Federal mandates such as those governing financial institutions and those governing all publicly-traded companies in the US.^{viii}

Risks



Risks to business functions should be categorized into

- **predictable risks** (such as hurricanes, floods, lack of raw material) which provide time to prepare
- **unpredictable risks** (such as tornadoes, sabotage, utilities failure) that typically occur without warning

Risk impact

Risk impact must be examined on several levels:

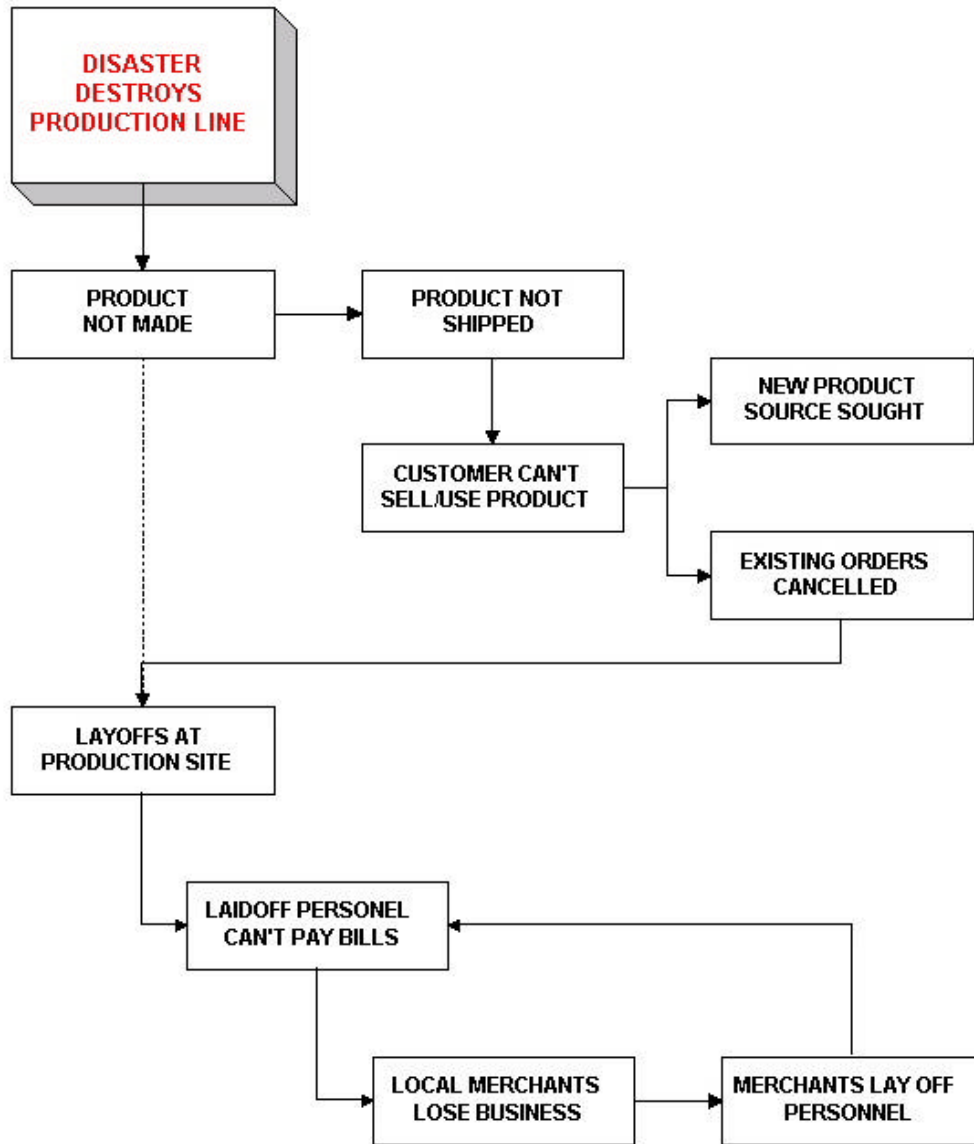
- impact on personnel, both at the site for which the plan is being prepared and at neighboring facilities
- impact on business

In the first case, there is the direct impact caused by death or injury.

There also is the impact caused by concern for family members’ welfare, particularly when the disaster condition is geographically widespread and when news of the family is delayed. Concern for job continuity also is a factor to be considered. As DR/BC planning matures, greater emphasis is being placed on human considerations. On the federal level, DR/BC planners should be aware of the Crisis Counseling Assistance and Training Program^{ix}, available following a presidential declaration of a major disaster under the Stafford Act.



The impact on the business usually includes the most obvious things: in a production environment, a disaster, as defined in [Definitions](#), easily could have a ripple effect similar to the following example.




Handling the risk

There are three primary options to handling a risk:

1. Avoid the risk
2. Mitigate the risk
3. Absorb the risk

Avoiding the risk means to take a proactive approach; to put measure into place to prevent a disaster condition from occurring. Some of the most common avoidance measures are:

- 
- maintaining AEC-5 or AEC-4 readiness status^x
 - establishing a policy that key personnel travel separately
 - installation of alternate power sources/supplies, typically Uninterruptable Power Supplies (UPSs) or local gasoline/diesel powered generators
 - maintaining duplicate records at a secure remote facility
 - stockpiling raw materials and finished product

Mitigation measures include:

- contracting for with company with similar equipment to utilize excess capacity (mutual aid agreements)
- establishing a second facility at a different location
- relocating equipment to a safer area in the same facility
- acquiring sufficient insurance to replace equipment (and maintaining up-to-date specifications for replacements)

There are times, however when a risk is **absorbed**; when a business decision dictates that a business function will be allowed to fail, or equipment associated with a business function is allowed to be “lost.” While this may *seem* contra-indicated for a DR/BC plan, in fact it is a valid option. The decision may be made due to obsolete equipment that is scheduled to be replaced, because a product fails to make its market share, or for any number of other reasons not related to a disaster or DR/BC planning.

In the same vein, there are things which are protected by commercial insurance, and things which will be replaced from available funds (typically “desktop” computer equipment).

6. Determine Business Recovery Strategies

Two things must be considered in the overall recovery plan: the **value to the business** - to save or not to save, and the **relationship to other businesses functions** - prioritizing the recovery.

Value to the business

The value to the business is the primary factor driving the prioritization. Is the function critical to the business’ continued operation? Are there a legal or contractual commitments? All functions are considered critical by the people performing those functions, but the bottom line is “what keeps the business in business?”

Relationship to other business functions

Related, albeit secondary, business functions also must be prioritized. For example, if a stockpile of raw material cannot be replenished due to transportation disruption, a production line can function for only a limited time (and even then, distribution will be prevented due to the same transportation problems).

7. Prepare and implement the plan

Developing scenarios for most-likely events

Predicable events

Floods are the most common disaster conditions^{xi}. Flood damage can result not only from rising waters, but from faulty structures (roof failures, wall and window damage during hurricanes, etc.), and water from fire suppression systems, among other sources.



In most cases, flooding is a relatively minor inconvenience and of limited geographic scope. In this case, “limited” may mean anything from to a single room or floor of a building to large low-lying areas with insufficient drainage to handle the waters. None-the-less, damage typically is localized.

Hurricanes, a frequent hazard in Florida and southern coastal states, bring both water damage from flooding (rain, storm surges) and wind damage, both directly to a facility (ripping away structure) and indirectly (hurling projectiles into facilities).

Since both floods and hurricanes normally are predictable, scenarios for these events should emphasize mitigation through facility site selection, business function physical location, and pre-event activities to transfer critical functions to a site outside the threatened area.

On a relatively minor scale, interruptions caused by equipment failure often fall within the “predictable events” category. Most commercial equipment is tested to determine a Mean Time Between (of Before) Failure (MTBF). In critical functions, equipment or equipment components nearing the MTBF should be replaced. The associated Mean Time To Repair (MTTR) determines what means, if any, must be put into place while the equipment is being restored.

Unpredictable events

Sabotage and civil disorder, the threat from within, are more difficult to predict and depend heavily on carefully selected mitigation options (such as personnel policies, surveillance cameras, security guards, and special equipment to limit access to secure areas) to reduce the threats. The degree of mitigation primarily is determined by the business function.

Most disaster conditions fall into the “unpredictable events” category. Weather and fire are the most frequent causes of unpredicted events and can impact a business in a number of ways ranging from disruption of communications services to blockage of access to, and egress from, a facility.

Most minor “unpredictable events” (such as utility failures, road closures, etc.) can be mitigated to a “nuisance” level through careful planning. Planners must, however, be careful to mitigate only those functions critical to the business and for the duration of the anticipated inconvenience. (There is no reason to purchase a back-up power supply to provide a 100kW supply if only 10kW is necessary for emergency operations.)

Knowing what to protect

Different business’ have different critical business functions.

The primary function of government is to provide for the protection and welfare of its citizens.

A manufacturing company’s most critical business function may be a production line; a company in a different business may depend on computer operations.

Protecting a production line might mean replicating the line elsewhere, and maintaining stocks of both raw materials and finished product.

Protecting a data center may simply mean storing software licenses, media, and backup media at a secure remote facility, or it might require setting up a hot site able to assume the primary data center’s functions with minimal notification.

Underprotecting a business can lead to its demise if it cannot recover sufficiently quickly to remain competitive. Overprotecting a business can lead to its demise due to unnecessary financial strain.

Recovery teams

Creating the team

Recovery teams must be carefully assembled. In order to achieve the greatest degree of effectiveness, the teams must

- include senior management - as with all DR/BC plans, the higher the level of management participation, the better the chance of plan success
- include manager-level personnel from all departments (business units)
- have both primary and alternate members from all business units
- have a clear understanding of the team's organization.

Identifying team members

Team members should be identified both by recovery team job function and by name.

The job function identifies the person's responsibilities and authority. This is a more-or-less static identifier. (As with all things relating to a DR/BC plan, it is "subject to change" as the plan is exercised and deficiencies are identified.)

The person's name is necessary to maintain a reach, or contact, list that includes the team member's contact information (address, primary and alternate phone, fax, and pager numbers, email, and any other communications devices).

Team assignments

Team assignments should be tailored, whenever possible, to the team members' strengths. The assignments must be thoroughly documented to preclude confusion as to members' roles during a disaster condition which normally is a hectic time.

Once assignments are made, both primary team members and alternates must train to become competent and comfortable with their duties.

Notification options and procedures

Notification options

Multiple notification options must be examined so if one method fails, an alternate is available.

While the telephone probably is the first choice, it must not remain the only choice. Depending upon the nature of the business for which the plan is prepared, several alternate methods may be desirable.

When considering alternate methods, make certain the alternates are free of any dependencies on other methods. (If the telephone lines are down at the disaster site, will there be anyone available to go elsewhere to call? Will the person be able - given roadway conditions in the area - to exit the disaster area to make the call? A business decision should be whether made to provide Recovery Team leaders (or all members) with cellular telephones or other wireless communications options.

Notification procedures

Who to notify is as critical as being *able* to notify. Both the person authorizing the notification - the person on the scene - and the person being notified, must be specifically identified in the Disaster Recovery Team organization chart.

Declaring a disaster

Who can declare

Who declares a disaster condition depends upon the nature of the disaster condition (one with warning or one without), but the declarer must be a person with the authority conveyed in the Disaster Recovery Team (DRT) organization.

In a 24*7 operation, the DRT shift leader is responsible to assess damage and to declare a disaster or, if the degree of damage is unclear, to alert the DRT leader to make an assessment. The leader, regardless of position, must have confidence in the DRT members making the damage assessments.

In a single-shift operation, and whenever the DRT leader is present, it is the DRT leader's responsibility to declare a disaster condition.

Response options

In addition to declaring a disaster condition, the Disaster Recovery Team (DRT) leader also determines how the disaster condition is to be handled. This is based on an assessment of the magnitude disaster or disaster threat. There are four general options.

Handle locally

If the disaster condition is local -- for example, malfunctioning equipment -- and if there are mitigation measures in place -- a backup unit -- the disaster condition is handled locally by transferring the function to the backup equipment.

Handle remotely with contracted personnel (shared resources)

The most cost-effective response to a disaster condition that requires remote operations to sustain the function is use of contract personnel and shared resources.

This typically is accomplished through mutual aid agreements, often by two or more divisions in the same company/government. There are a number of problems associated with mutual aid agreements (who controls the equipment, who has priority for the services, what services will be provided and who pays overtime, etc.); however, when a non-competitor has available surplus resources (e.g. computer processing and storage capacity), this is the low-cost option.

In order for this, or any, remote arrangement to work, however, the remote personnel must be included in the DR/BC planning.

Handle remotely with relocated personnel

This option is similar to handling the situation remotely with contract personnel and usually utilizes contract personnel services in the initial stages. Typically, selected members of the Disaster Recovery Team (DRT) travel to the remote facility where they assume responsibility for maintaining the critical functions while other DRT members remain at the disaster site to recover the facility.

Relocating personnel requires that the DR/BC plan include consideration for transportation, lodging, and subsistence for the DRT members at the remote facility. For extended stays, consideration also must be given to family unity (providing for family members at the remote site or providing for regular home visits for DRT members).

Handle remotely with contract, own personnel

This option often is utilized when a vendor service is used for data center backup. Vendor personnel assure the vendor-owned backup equipment is available and maintained; DRT members assure the critical functions continue on the vendor equipment. This is typically a vendor's "hot site" operation and requires special consideration to assure readiness^{xii}.

The relocation concerns cited for Relocated Personnel (above) apply in this case.



Hot sites, stand-by, cold sites

A **hot site**^{xiii} is a fully-equipped and staffed facility able to immediately assume specific functions which the impacted facility is unable to perform. This facility is the most expensive to maintain and is recommended for operations that must be fully functioning on a 24*7 basis.



A **stand-by site** is a fully-equipped facility able to assume, after a brief period, specific functions which the impacted facility is unable to perform. Since personnel are not on-site 24*7 prior to a disaster declaration, costs are substantially less than for a hot site.

A **cold site**^{xiv} is an unequipped, unstaffed facility - essentially a shell - than can assume, once all equipment is installed, configured, and tested, specific functions which the impacted facility is unable to perform. This site's success depends on the ability of the owner or vendors to get it quickly to an operational state. This option takes the longest time to make operational, but has the lowest maintenance.

Recovering the business



Assessing the damage

Depending on the nature of the disaster condition, it may be necessary to employ outside professionals to help assess damage to the facilities and functions.

With the exception of equipment and utility failures, most disaster conditions can cause damage to physical plants. The extent of the damage must be determined in order to make a business decision on how to handle the damage.

Production facilities damaged by a disaster condition also may require damage assessments by outside professionals.

Repairing the damage

There are three primary options to recover from damage.

- repair the damage/restore the damaged item
- replace the damaged equipment or facility.
- relocate (if a facility is damaged).

The repair/replace/relocate is a business decision that is based upon the damage assessment and various Federal, State, and municipal laws and codes (see [Business related codes](#)).

Repair or restore

Depending upon the type damage and the damaged material, specialists may be required to restore the damaged items. There are a number of sources listing specialists in a multitude of fields; some are highly specialized, others are more generalists. The sources of information should be included in the DR/BC plan as a "resources" appendix. In many cases, the earlier repairs/restorations start, the better the success rate. Repair/restoration costs normally can be off-set with commercial insurance and, occasionally, with government assistance. Both have the same "proof of ownership" requirements as cited in the following paragraph.

Replace

Equipment and facilities too damaged to repair or restore may be replaced. While many companies self-insure desktop equipment (computers, telephone instruments, etc.), most have commercial insurance coverage for major items (production equipment, data center equipment, etc.). An inventory of covered items should be included in the DR/BC plan as a "covered items" appendix, along with descriptions (and photographs, if appropriate), the insuring company, and insurance policy information.

Relocate

In the event there is substantial damage to the physical plant, an alternate rebuilding site may be suggested. This may be due to a business decision or to local ordinances which preclude rebuilding on the original site (see [Business related codes](#)).

Recovery declaration

When critical functions have been restored at the site impacted by the disaster condition, the facility's operation must be tested under increasing load to prove it is fully capable of handling the business requirements.

The Disaster Recovery Team (DRT) leader will, with executive management, declare the recovery function complete; business functions which were temporarily performed elsewhere or were performed under exceptional conditions will be returned to normal operation.

Depending upon the extent of the disaster condition's impact, recovery declarations may be made for less than total recovery. This is a business decision which should be made with input from the DRT members.

External advisors

In addition to in-house team members, DR/BC planners are well advised to seek input from external advisors. These advisors, who need not be privy to the entire plan, include (alphabetically)

- insurance providers
- municipal emergency planners/councils
- municipal planning and zoning personnel
- public safety departments (police, fire)
- suppliers, particularly hazardous materials suppliers

Additionally, some businesses may require input from hospitals, civil defense, and other specialty organizations.

Writing the plan

The DR/BC plan is created based on information described in Paragraphs 4, 5, 6, and 7. The plan may be manually created, or created using one of the many software tools available.^{xv}

8. Testing the plan



No DR/BC plan is complete until it is tested.

Testing shows where the plan must be revised; revisions are a normal part of a DR/BC plan's evolution.

However, testing can be expensive; both in actual dollar costs and in lost revenue. Testing also takes a toll on personnel, particularly when remote facilities are utilized.

There are, however, ways to greatly reduce the testing toll without an equally great reduction in the test's value. A number of commercial products offer ways to test a plan through simulation^{xvi}.

As much of the plan should be tested as possible; how much testing can be done remains a business decision.

9. Maintaining the plan

A DR/BC plan is a living document that must be maintained and constantly modified.

Personnel change; equipment is replaced; policies and procedures are modified. All these things must be reflected in the DR/BC plan if it is to remain valid.

The DR/BC plan should be reviewed on a regular schedule but not less than once-a-year. Interim changes are appropriate when an event occurs that has a major impact on the plan. What determines "major" varies by the operation the plan covers.



The plan should be tested after each major revision to assure that all “ripple effects” have been identified and accommodated.

10. Summary

The preceding is a **general** overview of a Disaster Recovery/Business Continuity plan’s development. There are a multitude of smaller steps that must be included in a successful plan, and substantial modifications to the general plan are required to make it suitable for specific applications.

DR/BC plans can be based on a boilerplate skeleton or template, but they must be “fleshed out” with a specific business operation in mind. This paper only provides the most basic DR/BC plan elements.

Bibliography

- i *Prove[It], Surviving a Computer Systems Disaster*, © 1999, Quantum Corporation;
http://www2.dlittape.com/ProveIt/exec_plan/index.htm
- ii DMR Consulting Group Inc., Florida Business Unit, 5110 Eisenhower Boulevard, Tampa FL 33634
- iii *Emergency Management Guide for Business & Industry*, Federal Emergency Management Agency; <http://www.fema.gov/library/bizindst.pdf>
- iv *Emergency Management Guide for Business & Industry*, *ibid.*
- v *Disaster Restoration Guide for Disaster Recovery Planners*, © 1998, BMS Catastrophe, Inc., Special Technologies Division, 303 Arthur Street, Ft. Worth TX
- vi *Business Resumption Planning*, p. I-1-4, © 1999, Auerbach
- vii *Business Resumption Planning*, p. I-1-2, *ibid.*
- viii *Business Resumption Planning*, p. I-1-4, *ibid.*
- ix *Disaster Assistance: A Guide to Recovery Program*, Federal Emergency Management Agency; <http://www.fema.gov/about/1-title.htm>
- x *Disaster Recovery or Disaster Tolerance: The choice is yours*, p. 72, Vol. 12, Issue 2, Spring 1999, Disaster Recovery Journal, <http://www.drj.com/>
- xi *A Citizen's Guide to Disaster Assistance*, p. 1-2, Federal Emergency Management Agency, <http://www.fema.gov/EMI/is7.htm>
- xii *Commercial Recovery Facilities: Selecting a Hot Site Facility*, p. 40, Vol. 11, Issue 1, Winter 1998, Disaster Recovery Journal, <http://www.drj.com/>
- xiii *Glossary*, Disaster Recovery Journal, <http://www.drj.com/glossary/glossleft.htm>
- xiv *Glossary*, Disaster Recovery Journal, *ibid.*
- xv *PC-Based & Mainframe Surveys*, p. 57, Vol. 11, Issue 3, Fall 1998, Disaster Recovery Journal, <http://www.drj.com/>
- xvi *PlanIt, LAN Recovery Planning System*, Peak Consulting, <http://www.peakcons.com/IncidentManager>, Strohl Systems, <http://www.strohl-systems.com/PreVision>, PreVision Design & Development, <http://www.previsiondesign.com/ESP>, Straylight Mulitmedia, <http://www.intergate.bc.ca/business/strylght/disaster.html>