Business Continuity Planning Guidelines

Texas Department of Information Resources

September 1999
Austin, Texas

Preface

State government addresses business continuity planning because of the consequences of not planning—financially, operationally, and politically.

The Information Resources Asset Protection Council (IRAPC) was a forum for agencies and universities to seek solutions in areas of resource protection through cooperative efforts and information sharing. In 1997, over ten agency and university representatives formed a special IRAPC team and began writing business continuity planning guidelines. These guidelines were presented to the Department of Information Resources (DIR) for publication. This document is a result of that special team's efforts.

The term "agencies" alone in this document also refers to state institutions of higher education.

Acknowledgments

Acknowledgment is given to the following individuals and their organizations for their cooperation and support in the development and authorship of this document.

The Information Resources Asset Protection Council
Contingency Planning Special Function Team

Phyllis Jamar, CBCP, Team Chairperson	Texas Department of Insurance
Claudette Clendennen	University of Texas Health Science Center at Houston
Rich Holmes, CBCP	Texas Rehabilitation Commission
Richard Landon	Office of the Attorney General
John Morgan, CBCP	Texas Rehabilitation Commission
Steve Schroeter	Texas Parks and Wildlife Department
Rick Torres, CBCP	Texas Department of Transportation
Robert Von Quintus	Texas Workers' Compensation Commission
Chuck Walts, CBCP, CRP	Texas Education Agency

Edited by Nena Young, CBCP, CRP, Texas Department of Information Resources, Richard Landon, Office of the Attorney General, and Barbara Bostick, State Office of Risk Management

Richard Fairlamb, Fairlamb and Associates, for Appendix 5: Example of a Business Continuity Plan Development Project *[Note: This acknowledgment was inadvertently omitted from the original published version and is therefore being inserted after publication.]*

"Tex" computer graphic created and contributed by Jay Galvan and Mike McCathern, Texas Water Development Board

Endorsed by the Texas Department of Information Resources, the Texas State Office of Risk Management, and the Texas State Auditor's Office

Disclaimer

Inclusions of references to vendor concepts or methods in these guidelines are for information purposes only. The appearance or absence of a vendor or product in this publication should not be construed as an endorsement or non-endorsement of a specific vendor, product, or company by the Department of Information Resources, the State Office of Risk Management, the State Auditor's Office, or any persons involved in the development of these guidelines.

Published by the Texas Department of Information Resources

Copies of this publication have been distributed in compliance with the State Depository Law, and are available for public use through the Texas State Publications Depository Program at the Texas State Library and other state depository libraries.

Contents

Introduction

Business continuity planning provides a quick and smooth restoration of operations after a disruptive event. Business continuity planning is a major component of risk management. Business continuity planning includes business impact analysis, business continuity plan (BCP) development, testing, awareness, training, and maintenance.

A business continuity plan addresses actions to be taken before, during, and after a disaster. A BCP spells out in detail what, who, how, and when. It requires a continuing investment of time and resources. Interruptions to business functions can result from major natural disasters such as tornadoes, floods, and fires, or from man-made disasters such as terrorist attacks. The most frequent disruptions are less sensational—equipment failures, theft, or employee sabotage. The definition of a disaster, then, is *any incident that causes an extended disruption of business functions*.

Traditionally, disaster recovery planning has focused on computer systems. Because mission-critical functions inevitably depend on technology and telecommunications networks, rapid recovery of these is of little value without also recovering business unit operations. Mainframe and minicomputer systems usually have reliable recovery plans. Today, however, many critical applications have migrated to distributed, decentralized environments with less rigid controls. Recovering functional processes includes more than just information systems—consideration needs to be given to such items as 800 and long distance service, locations for employees to work, the salvage of building contents, and so forth.

As with an insurance policy, it is hoped that a business continuity plan is never needed for a real disaster. Keep in mind that a BCP not maintained can be worse than no plan at all. An agency's ability to recover mission-critical processes, resume operations, and eventually return to a normal business environment can be considered a major asset. Thorough planning can reduce liability, disruption to normal operations, decision making during a disaster, and financial loss. And equally important to state government, it can provide continued goodwill and service to the state's citizens.

Determining Scope and Readiness

The purpose of this section is to determine what information is needed to begin business recovery planning, and how to determine the scope of the planning effort based on this information.

The commitment of management is essential for the business recovery effort to succeed. Management commitment can be recognized when

- A sound impact analysis is funded, the results of which are read, understood, and acted on by management deciding to use a strategy based on likely impacts to the organization.
- Comprehensive planning involves all program and technical management's clear accountability for the continuation of the areas that they manage. The effort culminates in a written plan that is specific, credible, and candid regarding its constraints, weaknesses, and vulnerabilities.
- An ongoing exercise and maintenance program is developed that ensures the viability of the BCP.

A practical approach is one that plans for the worst-case-scenario—including:

- Loss of access to the facility,
- Loss of access to information resources (systems, networks, data), and
- Loss of skilled or key personnel who perform critical processes.

Just about any event could result in these losses. A practical plan is based on the input analysis, which details the element of recovery by priority and timeframes. This approach provides procedures for dealing with less devastating events as well as "smoke-and-rubble" disasters.

Don't concentrate on what can bring you down, but on what can bring you back up.

Most recoveries focus on the most critical functions by

- Moving selected personnel to an alternate facility.
- Using alternate information resources and other office equipment.
- Repairing/replacing equipment or making minor repairs to the home site.
- Returning to the home site in a fairly short time.

The organization cannot meet its mandated missions without its support functions. Recovery must involve the entire organization—facilities, administration, accounting, information systems, personnel, and most importantly, the business functions that perform the missions. All functions must interact with each other for optimum recovery.

The business recovery process includes determining critical functions, identifying the available resources, establishing the level of support needed, and determining the methods to be used.

The parallel between the business recovery planning effort and other business planning efforts is useful to all managers who are called on to contribute to the business recovery effort.

- From a business perspective, management must be aware that the effort can contribute something to the organization that would not be possible otherwise.

Thorough planning, for example, can provide management with a complete picture of the organization's processes and their dependencies.

- Projects proceed with a careful analysis of needs.
- With analysis complete, the design is created.
- When the design is approved, resources are committed to develop the product. Costs must be clearly defined.
- Upon completion, testing performance and integrating changes refines the product.
- Support and maintenance tasks keep the product current and relevant to the business.

An effective method for developing the scope of the plan is to focus recovery efforts on the major mandates of your organization. Each business recovery plan should provide action steps to recovery from

- Loss of physical or electronic access to computer centers, information resources, offices, or multi-use facilities maintained by the state agencies and resources therein.
- Loss of key information needed for the organization to function.
- Loss of key personnel involved in any business function, use of information resources, or the decision-making function, which could have intolerable impacts if not recovered in a determined amount of time.
- Testing and maintenance of the recovery process reflecting the inevitable changes in growth and functionality of the organization.

Performing a readiness audit determines how prepared an organization is to respond to a disaster. The readiness audit differs slightly from risk assessment/analysis. The audit determines what resources are already available for use in the business recovery

planning effort and what resources are missing, rather than determining threats to assets and subsequent frequency and severity of threat.

How to Perform a Readiness Audit

1. Check for the existence of the following documents or information and review:
   - Emergency Procedures
   - Fire Protection Plan
   - Safety and Health Program
   - Finance/Purchasing Procedures
   - Hazardous Materials Plan
   - Process Safety Assessment
   - Vital Records Management
   - Risk Analysis/Assessment
   - Capital Improvement Program
   - Hazard Materials/Waste Disposal
   - Alternative or Manual Procedures
   - Evacuation Plan
   - Environmental Policies
   - Security Procedures
   - Facility Closing Policy
   - Employee Manuals
   - Risk Management Plan
   - Mutual Aid Agreements
   - Hotsite Agreements
   - Coldsite Agreements
   - Internal Disaster Plans
   - Disaster Recovery Plans for Information Resources
2. Based on the review, ask the question: How would your organization resume operations after loss of access to your facility, loss of access to your information resources (IR), or loss of key personnel?
3. Perform an informal survey of technical and business managers and ask them if they know what to do if your organization lost access to the facility, lost access to your information resources, or lost a number of key personnel.
4. Have any audit findings been reported from internal or external auditors?
5. Would most individuals know how to report or respond to an event?
6. If policies relative to recovery efforts are in place, who knows about them?
7. Has priority ever been assigned to the order in which business functional units are recovered?
8. Do people know if they have recovery responsibilities? Are program managers aware of their owner and user security responsibilities?
9. Has the IR organization met with any program areas to discuss business recovery planning efforts?
10. Has any business recovery planning information been published by any of the following areas of your organization:
    - Risk Management
    - Public Relations
    - Program Management
    - Security
    - Human Resources
    - Management Information Systems/ Information Technology

11. Has testing been done to see how people would react during a recovery effort in the following areas:
    - Senior Management
    - Security
    - Risk Management
    - Auditing
    - Service Bureau
    - Management Information Systems/ Information Technology
    - Internal Departments
    - Vendors
    - Telecommunications
12. Check to see if
    - Computer backups (PC, LAN, mainframe) are being taken off-site according to policy;
    - Alternate work locations are available;
    - Items required to be off-site are really there;
    - Security measures are being followed;
    - Emergency equipment (generally UPS, batteries, etc.) is working correctly;
    - Emergency lighting is in good working order and in the correct places.
13. Create an awareness by
    - Copying articles and circulating to people mentioned in number 11 above;
    - Writing memos;
    - Getting involved in employee training/orientation;
    - Working with auditors and risk managers;
    - Providing management with realistic information on the status of the organization's ability to withstand an interruption or disaster.

Business Recovery Responsibilities

Texas Administrative Code (1 TAC 201.13(b)) defines specific responsibilities for information resource asset ownership, custodian, and user responsibilities. Business recovery, a key component of asset protection, requires responsibilities significantly different from those of the information security function. The following guidelines for business recovery outline the roles and responsibilities associated with the planning activities.

The coordinator chosen to lead or manage business recovery planning needs to be familiar with all of the agency's business functions and be able to cross the organizational and budgetary lines. Assigning the Information Resources Manager (IRM) to the role of business recovery coordinator may or may not be the appropriate choice.

Executive Management

The agency head must assure that the agency's resources and information assets are protected, including planning for recovery from the effects of damage or destruction. The agency head is responsible for establishing and maintaining a business recovery planning program within the agency and appointing appropriate personnel to administer information resource and business recovery planning.

Typically, heads of agencies are responsible for the following:

1. Enforcement of state-level disaster recovery and business recovery policies.
2. Establishing and maintaining a business recovery program, including an impact analysis process that identifies critical business processes.
3. Establishing and maintaining internal policies and procedures that provide for the recovery of personnel, information technology, facilities, software, and equipment, and the business functions that they enable.
4. Assigning program managers to administer business unit and information resources recovery responsibilities for all critical business unit and information resources within the agency.
5. Ensuring the preparation and maintenance of the agency's business recovery plan for the continuation of critical business functions and information support services in case of a disaster.
6. Ensuring agency compliance with the DIR standards by describing disaster recovery requirements in the agency strategic plans in accordance with 1 TAC 201.13(b).
7. Ensuring agency compliance with state information systems audit requirements.

8. Ensuring participation at all necessary levels of management, administrative, and technical staff during the planning, development, testing, modification, and implementation of disaster recovery and business recovery policies and procedures.

Program Management

Agency program managers have ownership responsibility and management authority for the personnel, information assets, equipment, and property used in fulfilling the goals of the program(s) under their direction.

Program managers need to work in cooperation with the agency business recovery coordinator, acting on behalf of the agency head, for the purpose of recovery of all critical business functions and information resources within the agency.

Program managers should assign custody of program assets to appropriate staff and ensure the staff is provided appropriate direction to implement the defined procedures.

Typically, program managers should

1. Define the specific processes and resources that need to be in place to minimize the impact of interruption; assign responsibilities.
2. Participate in the agency's impact analysis process to identify business functions required by law or otherwise critical to the mission of the agency and the State of Texas.
3. Ensure participation between the program staff, technical staff, and the business recovery coordinator by identifying and selecting appropriate, cost-effective strategies and procedures to recover business functions and information assets.
4. Ensure the proper planning, development, and establishment of recovery policies and procedures for all files or data bases supporting critical functions for which the program has ownership responsibility, and for physical assets assigned to and located in program area(s).
5. Formally assign custody of program assets to appropriate managers and ensure direction is provided to implement the defined recovery plans, strategies, and procedures.
6. Establish all recovery procedures necessary to comply with these guidelines for recovery of critical agency missions, which would have intolerable impacts on the state if lost.
7. Ensure contractual agreements exist, based on impact analysis, for recovery of the state's mission-critical business functions and information resources, where technical services are outsourced to another agency or private firm.

Program managers are accountable for recovery of their business functions. *Recovery planning should become a part of their unit goals and performance evaluation.*

Technical Management

Technical managers have a role in business recovery. Technical managers include Information Resource Managers (IRMs), data processing directors, data center managers, and network directors. These individuals have custodial responsibilities, provide information services, and have oversight or support responsibility for information resource assets that support business functions.

Typically, technical managers need to

1. Provide the necessary technical support services to define and select cost-effective recovery strategies, policies, and procedures.
2. Ensure the development and documentation of recovery strategies and procedures for critical business functions as defined by the owners of the information.
3. Develop and implement adequate backup and recovery procedures for all critical data and software in the facility.
4. Implement and maintain a recovery plan for information resources resumption in cooperation with agency management, the business recovery coordinator, program managers, custodians, and the assigned owners and users.
5. Monitor the recovery testing and develop the reports and reporting procedures in accordance with the requirements of the DIR, program areas, and auditors.
6. Coordinate the business functions to identify the information resources (facilities, personnel, data, voice communications, equipment) required to support the IR-dependent processes for mission-critical needs.

This can be based on the resource dependencies analysis.

7. Identify, evaluate, and arrange for the acquisition of alternative information resources and recovery services as required to recover the critical business functions as a custodial role.
8. Develop appropriate information resource recovery strategies based on the results of the analysis and business process study.

It is recommended that *recovery planning become part of technical managers' goals and performance evaluations* if those managers provide technical support of critical business functions.

Business Recovery Coordinator

In many agencies, recovery planning is assigned as a sub-function of another full-time position within the organization. However, assignment of the duties is significant

because of the function's unique and critical nature. The function crosses organizational and budgetary lines. It combines business and technical information roles and responsibilities and is critical to the continuation of the agency's mission.

Assignment of business recovery responsibility includes authority from the agency head to act as a liaison between program management and technical management for the purpose of recovery planning. The function should be positioned on the agency organization chart with direct access to the executive office, as is the internal auditor.

Planning as a full-time assignment may be justified, depending on the size and complexity of the organization, and the importance of the agency's mission to the state.

The primary focus of the business recovery coordinator is to oversee a viable and tested business recovery plan that demonstrates to management the agency's ability to continue critical business functions following a disruption of services. Maintenance of the plan is ongoing, reflecting changes in the agency and its mission. Testing is conducted regularly to ensure the viability of the plan. Training also occurs on a regular basis to assure agency-wide awareness of the business recovery function.

Typically, the business recovery coordinator

1. Coordinates the planning activities of team members.
2. Develops an initial budget and informs senior management of any changes.
3. Oversees the identification and review of critical tasks that are essential during recovery, based on input from program and technical management in the business impact analysis process.
4. Establishes an ongoing training program to promote agency-wide awareness of the recovery function.
5. Establishes a timetable for regular review and updating of plans, resources, and procedures to ensure that changes to critical procedures, functions, and documentation are reflected in the plan.
6. Coordinates monthly, quarterly, semi-annual, and annual testing of the plan as needed, reporting results to management.
7. Establishes a standards program that ensures changes to critical procedures, functions, and documentation are reflected in the plan. Assures that contact is maintained with all personnel as necessary to keep recovery support considerations current.
8. Maintains contact with vendors to assure support during a recovery effort.
9. Acts as a liaison for contingency planning issues between information resources and other business units, including auditing.
10. Meets regularly with recovery teams to review responsibilities required during a recovery effort.
11. Maintains contact with city, county, state, and federal emergency organizations that may be involved during a recovery effort.

12. Provides input, support, and coordination to other departmental areas for projects that relate to contingency planning (e.g., updating documentation, creating procedures, evaluating security systems).
13. Researches, evaluates, and recommends internal and external solutions to business recovery problems.
14. Maintains contracts for alternate facilities and/or services.
15. Provides input for performance reviews of contingency planning staff.

The recovery coordinator's role is coordination with and among program and technical managers. These managers implement and carry out the recovery.

Internal Auditor

Typically, internal auditors

1. Examine the agency's business recovery plans for compliance with state policies, standards, and guidelines on an annual basis.
2. Ensure necessary controls are followed during an actual emergency.
3. Report findings to management.
4. Follow up to ensure compliance with findings.

Risk Manager

An agency's risk manager may be assigned to overall compliance with the State Office of Risk Management's requirements. Coordination between risk management, information resource recovery, and business recovery planning activities is highly recommended. The organization's risk manager may be placed as part of the other support functions in the organization chart. The risk manager, including information resource management, has the bulk of recovery responsibilities following an interruption to the overall operations of the organization.

Records Management

Most agencies use records management to archive state records, a service provided by the state library. The state library can also offer off-site storage for retrieval of critical, vital records for recovery purposes. Rapid turnaround time is available. This is an often overlooked resource for records that are vital for recovery, but may be protected off-site.

The state archive personnel also have excellent working knowledge of disaster recovery and business recovery methodologies.

Recovery Teams

Recovery teams should be developed specific to the contingency planning needs of each agency. Team development depends on the size and complexity of the tasks that need to be accomplished for planning and recovery. The following teams reflect the tasks at hand.

Administration. This team reports to the command center to support the emergency management team and the business recovery coordinators; provides administrative support services, including travel and lodging, petty cash disbursement, notifications to customers, and preparation of all reports for the recovery operation.

Business Function Recovery. This team responds to and manages any serious interruption to specific business function operations; develops recovery strategies and procedures based on a business impact analysis.

Command Center. The command center team activates the facility to be used for assembly of the emergency management team, help desk team, administration team, and the business recovery coordinators when a disaster has occurred. They are also responsible for the initial distribution of supplies, forms, and off-site boxes stored at the warehouse. This team is made up of warehouse and facilities personnel.

Damage Assessment. This recovery team assesses the damage of the disabled facility and its contents, both preliminary (immediately after an event) and comprehensive assessments. Activities are coordinated with the business recovery coordinator, IS recovery coordinator, emergency management, and facility preparation team. Members of this team include General Services Commission (GSC) building engineers, data services and risk management personnel, and any related vendors or technical experts.

Hazmat teams are allowed in facilities first when hazardous materials are involved. Damage assessment teams must wait until access has been granted to the damaged facility.

Emergency Management. The emergency management team provides overall management to all recovery teams; authorization for disaster declaration; business recovery functions for all operating business units; guidance for all restoration activities; agency funding and expenditure arrangements; and, public relations information.

Emergency Purchasing. This team coordinates the replacement (purchase and/or lease) of all damaged equipment at the disabled facility as well as equipment required for alternate operations. They also coordinate the delivery and installation of such equipment at the alternate facility. This team handles the procurements for all information resources, general office needs, and facilities requirements. The team

may also request a suspension of purchasing rules and regulations to facilitate recovery.

Equipment Installation. This team controls the installation of all terminals, PCs, and printers at the alternate site. Personnel for this team are primarily from PC/LAN and telecommunications support areas. This team interfaces with all business units and works directly with the emergency purchasing and facilities preparation teams.

Executive Management. The organization's (agency's) executive management communicates support of the business recovery process by issuing a formal policy statement; periodically reviewing the recovery assumptions, potential loss assumptions, strategic considerations, and definitions of resumption priorities. Executive management ensures that adequate resources are devoted to the project by approving recovery strategies, possible alternatives, funding, and ongoing maintenance.

Facilities Preparation. The facilities preparation team coordinates and directs all activities necessary to restore, build, and/or lease a replacement building. The team reviews business unit requests for office space; provides alternate site facilities to continue critical business functions; and, participates in damage assessment to the affected facility.

Finance. The finance group oversees proper authorization and support of expenses during emergency procurement.

Information Services. The IS team maps the recovery of the information resources (mainframe computer and associated services, telecommunications and connectivity, LANs, WANs, and PCs) for business function recovery at an alternate site. The organization may have a central computing center and/or distributed systems which would dictate the size, complexity, and areas of responsibility of the teams. The basic responsibilities include the following:

- Applications—restores and supports application systems at the recovery center and defines data files retention periods for off-site storage.
- Data Base Administration—restores all critical data bases and evaluates their integrity; closely coordinates file synchronization and balancing conditions with the applications team prior to resuming production processing.
- Data Security—maintains data security of the electronic records and files throughout the recovery operations. Data security entails system access via passwords. The team is functional throughout the entire recovery effort.
- IS Recovery Coordinator—coordinates all activities of the recovery teams for the agency's central computing center and works closely with the business recovery coordinator and the other teams. Depending on the size of the organization, this function may also be the business recovery coordinator.

- Help Desk—processes all end-user inquiries and requests concerning the recovered computer systems during the recovery effort.
- Mainframe Distribution—controls all printed output. Output created by outside vendors is controlled by this team. This team interfaces with all business recovery teams and the operations team.
- Network—restores both voice and data critical circuits and maintains a backup telecommunications network. The team interfaces closely with business recovery, systems software, operations, and facility preparation teams.
- Operations—supports restoration of the mainframe utilities, critical applications and databases, I/O controls, and schedules all production applications. Most team members are staff from central computer operations.
- Off-site Storage—retrieves all required electronic media from the off-site storage location and transports it to the recovery center. Reestablishes or maintains an alternate off-site storage location for rotation of electronic vital records throughout the recovery effort.
- System Software—restores the operating system and all subsystems at the alternate recovery center. The team also prepares the operating system configuration to be used in the alternate site and restored primary home site.

Legal. The legal team ensures that legal issues or procedures related to potential agency liabilities are addressed in the plan.

Physical Security. This recovery team provides physical security for all personnel, the buildings, and all alternate sites.

Public Relations. The public relations team provides accurate, essential, and timely information to employees, employees' families, the media, and customers about what has happened and how the recovery plan is working. This team ensures the appropriate spokesperson addresses environmental, health, and safety issues.

Team Leaders

A team leader is assigned from each business unit to be responsible for coordinating all team planning, testing, and recovery activities. Ideally, team leaders are members of first-line management or project leaders with strong leadership and organization skills, and are detail-oriented with a basic knowledge of the business unit's functions. They are responsible for all liaison activities between the agency's recovery coordinators and other team leaders.

Team Members

The skills and abilities of the combined team members must cover a wide range of responsibilities, many of which are dictated by the business function(s). Ideally, team members are supervisors who can effectively invoke a business unit's recovery process in the event of a disaster. Team members are responsible for researching their respective parts of the plan and for meeting deadlines. It is recommended that one team member serve as a scribe to create the plan documentation. If the plan is executed, the scribe maintains a log of recovery activities and expenses. Also, one team member should be responsible for the maintenance of any off-site storage.

Analysis and Strategy Selection

Effective analysis is essential in plan development, strategy selection, and reduction of recovery costs. Impact analysis involves the owner/business function/program manager's input to understand precisely what the agency risks losing should there be a disruption or disaster. While overall responsibility lies with the agency head, information needed for recovery comes from all levels of management. The IS organization alone cannot provide that information. The effort needs to be a "meeting of the minds" that results in identifying, qualifying, and quantifying the terms "critical" and "intolerable impacts." Only the owner can identify, quantify, and qualify these impacts.

Impact analysis ensures that the intolerable impacts are the main consideration in defining the direction, scope and appropriate recovery strategies for plan development. Simply put, the shorter the time in which the impacts become intolerable, the hotter the strategy (*most* resources in place, ready to use). Conversely, if the impacts are tolerable for two weeks or more, then a colder strategy (resources identified, but not in place) is indicated.

One of the lesser known advantages of performing a business impact analysis (BIA) is that the awareness level of many of the organization's employees rises significantly as BIA interview questions and "what if" scenarios are discussed. This can have an advantage in speeding the progress of the project and helps to gather consensus and support from areas of the organization which otherwise would not have understood the importance of enterprise-wide recovery plan development, testing, and maintenance.

Impact analysis is often confused with risk assessment. Risk assessment is associated with determining the potential losses of a threat vs. the cost of the protective measure against the value of the asset. It is related to determining how much to spend on prevention and protection. Although risk assessments are a very important step in the analysis, all of the information needed for recovery planning does not result from this one step.

The current rule assumes that critical applications and business functions are known before conducting the risk analysis. The following table compares the conceptual differences between risk analysis and impact analysis:

Risk Analysis	Impact Analysis
To what lengths do we go to protect information resources?	How long can we tolerate NOT having access to information resources?
Weighs the losses of information resources in the absence of security controls against the cost of implementing the control.	Weighs the intolerable effects of the loss to the organization against the cost of reacting to the loss over time.
Evaluates vulnerabilities to an asset and probabilities of occurrence.	Evaluates the effect of an event over a period of time.
Specific threats and causes.	Cause of the loss is irrelevant.
Protective and counter measures.	Recovery strategy.
How can we be proactive?	How are we going to react and recover?
Prevents and protects as much as is economical.	Provides information for an efficient and effective recovery plan.

Business Impact Analysis

In preparation for conducting a business impact analysis (BIA), the process must include the following considerations:

- Executive sponsorship of the effort.
- Support and involvement of senior management.
- An unprecedented study of the organization.
- A collective undertaking with those whose continuity is sought are major contributors to the process and are intimately involved in the assessment of their value.
- Results of a BIA position each business and support function in the order for recovery based on organizational knowledge.
- Interviews of people from all the functional and support areas who know the business processes and can respond to a structured questionnaire quantitatively.
- Interviewees range from those who feel the organization “cannot survive without me” as well as the ones who “hold the organization together with their bare hands.”
- BIA conveys the needs of the organization and what the impacts would be if critical functions were not recovered in a timely fashion.
- BIA results are the foundation and cornerstone of the plan and strategies selected to use in the event of a disaster.

BIA Questionnaire Development

In preparing the questionnaire, the metrics used should be decided on and followed consistently. Even if automated tools are used, it is recommended that some of

interviews be conducted face-to-face with the understanding that there will be iterations and opportunities to fine tune the responses. The questionnaire determines actual impacts to an organization as if it were experiencing an actual interruption. For consistency in responses and ease of comparison

- Describe business function being interviewed.

  Example: Negotiates and administers contracts, 10 personnel, under the deputy director, located in the Brown Building, third floor.

- Use consistent critical timing elements.

  Example: 24 hours, 2 days, 5 days, 1 week, 2 weeks, more than 2 weeks.

- Use orders of magnitude for dollars, population, and other quantifiers.

  Example: $10K, $50K, $100K, $500K, $1m, $5m, etc.; minor, medium, major.

Information provided by the BIA Questionnaire

BIA questions beginning with *WHEN would the disruption*

- First become noticeable by the average state citizen? (Include private sector, federal government, state agency, political subdivisions, internal functional area, and any other entity that would be affected.)
- Result in unusually large number of complaints or severe criticism? (List positive actions to reduce complaints and criticism.)
- Substantially increase, decrease? (State the time period(s) and the cause.)
- Be countered by positive action to reduce complaints? (Explain the actions needed.)

BIA questions beginning with *WHEN would the disruption impact*

- Current revenue generation or control? [What is the source and amount?]
- Future revenue generation or control? [What is the source and amount?]
- Infrastructure support (power, water, sanitation, telecommunications) responsibilities your agency might have?
- A number of citizens or a specific subset of population served? (How many?)
- Public safety or health?
- Environmental conditions?
- Statutory and legal obligations (legislative or federal mandate to perform the function under any circumstances)?
- Exposures to legal liabilities if a function was not performed?
- Contractual obligations? What would be the financial penalty?

- Public access to information?
- Public image of your organization and its leadership?

Analysis Report Format

- The structured questionnaire allows data collection in a format that enables direct comparison of results.
- Patterning will emerge that defines the impacts in the loss categories. The most critical functions will group accordingly.
- The report should provide prompt and specific feedback of the impacts with time frames to the interviewees and executive management in meaningful, recovery-related statements. The business impact analysis process and feedback increases heightened awareness of the need for continuity that supports its effective implementation and allows for adjustments over or under estimated responses.

The resulting clarity of perception of the agreed, calculated costs of disruption will provide a powerful stimulus to ongoing executive support in the continuity planning process. (Gartner Group)

Example: Major criticism would occur within three days from the private business sector.

Example: Vendors could insist on a 1½ to 2% late payment ($15-20K) penalty in 30 days.

Example: The inability to make bank deposits would result in $250K loss of interest payments in eight hours.

Example: A major public relations exposure would occur in as little as three days to those entities that are waiting permits.

Fine Tuning Priorities

Information collected from the business impact analysis provides a subset of functions that are critical. To fine tune the priorities of these functions, a business process study is required. The basis of this analysis is collected early in the questionnaire under internal functional areas. This analysis looks at where work flows begin and end and gets down to the level of business processes and how each functional area of an organization is connected.

Suppose business function **X** is considered the most critical, based on the business impact analysis. However, business function **X** depends on inputs from business function **Y** before work can begin. Therefore, the process performed by business function **Y** must be recovered before business function **X** can begin work.

Determining Resource Dependencies

The purpose of this part of the questionnaire is to document what resources the essential work conducted by a particular function depends on. It is recommended to identify resource dependencies for at least each critical and essential business function. The goal is to determine the very minimum of resources required to perform only the most critical or essential processes and tasks.

During recovery, resources (i.e., phones, faxes, PCs, printers, etc.) should be shared among all of the critical and essential business functions to a greater degree than in normal business. When all the dependencies are known, tabulate them together according to the resource and the time period in which they are needed to result in the minimum resource requirements—the basis of strategy selection.

For each critical business function interviewed, ask the following question for each resource. Add the details based on the function's specific requirements.

Is critical or essential work DEPENDENT on *key job functions?*

Job Function	Skills	Task	Quantity	Time
What Supplies Are Required?				
Service Dependency (Major, Medium, Minor)				
Actions to Reduce Impacts?				

The number of key personnel should drive the quantity and time needed for most of the other resources listed below.

Is critical or essential work DEPENDENT on the *telephone?*

Job Function	Telephone Specifications *	Volume	Quantity	Time Needed
What Supplies Are Required?				
Service Dependency (Major, Medium, Minor)				
Actions to Reduce Impacts?				

* Voice, data, incoming, outgoing, voice mail, call distribution, voice response, conference, multi-track voice, recorder, video, speaker phone; peak times of day, week, year.

Is critical or essential work DEPENDENT on the *fax?*

Job Function	Fax Specifications *	Volume	Quantity	Time Needed
What Supplies Are Required?				
Service Dependency (Major, Medium, Minor)				
Actions to Reduce Impacts?				

* Incoming, outgoing, advanced capabilities, peak times of day, week, year.

Is critical or essential work DEPENDENT on a *personal computer?*

Job Function	PC Specifications *	Quantity	Time Needed
Service Dependency (Major, Medium, Minor)			
Actions to Reduce Impacts?			

* Manufacturer, model, type of work performed, software/hardware requirements, PC connectivity.

Is critical or essential work DEPENDENT on *printer(s)?*

Job Function	Printer Specifications *	Quantity	Time Needed
Service Dependency (Major, Medium, Minor)			
Actions to Reduce Impacts?			

* Manufacturer, model, type of work performed, software/hardware requirements, PC connectivity.

Is critical or essential work DEPENDENT on a *LAN or WAN?*

Job Function	LAN / WAN Specifications *	Quantity	Time Needed
What Supplies Are Required?			
Service Dependency (Major, Medium, Minor)			
Actions to Reduce Impacts?			

* Manufacturer, model, quantity, type of work, software/hardware requirements, connectivity.

Is critical or essential work DEPENDENT on a *midrange computer?*

Job Function	Specifications *	Quantity	Time Needed
What Supplies Are Required?			
Service Dependency (Major, Medium, Minor)			
Actions to Reduce Impacts?			

* Manufacturer, model, quantity, type of work, software/hardware requirements, connectivity.

Is critical or essential work DEPENDENT on a *mainframe computer?*

Job Function	Mainframe Specifications *	Quantity	Time Needed
What Supplies Are Required?			
Service Dependency (Major, Medium, Minor)			
Actions to Reduce Impacts?			

* Manufacturer, model, quantity, type of work, software/hardware requirements, connectivity.

Is critical or essential work DEPENDENT on any *UNIQUE equipment?*

Job Function	Manufacturer / Model *	Specifications	Quantity	Time Needed
What Supplies Are Required?				
Service Dependency (Major, Medium, Minor)				
Actions to Reduce Impacts?				

* Calculators, copiers, typewriters, transcribers, audio recorder/Dictaphone, audio/visual, etc.

Is critical or essential work DEPENDENT on any *internal work group?*

Work Group	Description / Location *	Type of Work	Volume	Time Needed
What Supplies Are Required?				
Service Dependency (Major, Medium, Minor)				
Operational Dependency (Major, Medium, Minor)				
System Dependency (Major, Medium, Minor)				
Actions to Reduce Impacts?				

* Number peak times of day, week, year.

Is critical or essential work DEPENDENT on any *external computer system(s)?*

Organization / System	Description / Location *	Type of Work	Volume	Time Needed
Terminal Connedtivity? Quantity?				
Service Dependency (Major, Medium, Minor)				
Operational Dependency (Major, Medium, Minor)				
System Dependency (Major, Medium, Minor)				
Actions to Reduce Impacts?				
Does this EXTERNAL SYSTEM Have A Business Continuity Capability? If Yes, How Long Before Resumed?				

* Number peak times of day, week, year.

Is critical or essential work DEPENDENT on any *vital records?*

Job Function	Vital Record Name Description / Location	Normal / Recovery Source	Normal / Recovery Media *	Time Needed
What Supplies Are Required?				
Service Dependency (Major, Medium, Minor)				
Operational Dependency (Major, Medium, Minor)				
Actions to Reduce Impacts?				

* Paper, microfilm, fiche, PC/LAN, PC, mid-range, mainframe, optical, Rolodexes, directories, etc.

Organizing and Tabulating the Results

The results of the resource dependencies may be formatted by listing all the resources that are needed down one column. Across the top of the table, have columns for the time periods in which recovery must begin. Fill in the matrix matching the quantity of the resources needed with the time period in which they are needed. Complete a matrix for each function and total all resource needs in a similar matrix.

For example:

Resource Needs for Business Function X	Day 1	Day 2	Day 3	Week 1	Week 2
Personnel	3	5	7	18	24
Telephone	1	3	5	12	15
PCs	1	2	4	12	20
Printers	1	1	2	6	8
LAN / WAN connections	0	2	4	10	20

Review all the resource requirements and look for opportunities to share resources and reduce the overall amount.

Combine all resource needs and the time they are needed into a master matrix for strategy selection, and document what is needed and when it is needed.

Resource Needs For Business Functions X, Y, Z	Day 1	Day 2	Day 3	Week 1	Week 2
Personnel	12	15	28	72	96
Telephone	4	12	20	48	60
PCs	4	8	16	48	80
Printers	2	2	3	4	6
LAN / WAN connections	0	2	10	30	80

The resource dependency analysis shows what is needed when, and how much impact would justify how hot, warm, or cold your strategy needs to be.

Foundation of the Business Recovery Plan

Following an interruption, the losses become intolerable within a specific period. This is the recovery window. Selection of the correct strategies should be based on the recovery window resulting from the impact analysis process. Therefore, if intolerable impacts would occur in one week or less, a hotter recovery strategy is indicated. A hot strategy is one that requires most of the recovery resources to be already in place and ready to use. If intolerable impacts would occur after longer periods, a colder recovery strategy is indicated. A cold strategy is one in which recovery resources are put in place following an interruption. Even with a cold strategy, it is critical that the recovery resources are identified, listed, prearranged, and preplanned as to how/where they will be acquired and how/when they will be delivered, installed, and used. Usually, a combination of recovery strategies should be planned.

Business Recovery Strategies

When evaluating options for business function recovery at an alternate location, certain criteria can be used. Ensure the strategy is available and usable within the recovery

window. The alternate location should be of sufficient distance from the normal location to prevent it from being impacted by the same event. Logical first choices would be other locations of the organization, such as training facilities. Remote locations have the advantage of being protected from regional events, but may cause logistical problems of moving groups of people and establishing an alternate routing path for networks. Some entities are electing to look for available space when the need arises, which may be suitable for simpler recovery requirements and longer time frames.

Whatever alternate site is selected, considerations must be made for site preparation to suit the needs of the business function. Preparing a site involves many of the same issues as moving an office, but implemented within a much shorter time frame.

A starting place is to inventory the current site's characteristics, and document in a form or checklist to use when evaluating the suitability of other sites.

The ability to quickly contact vendors and other sources for specific recovery resources is extremely important. Prepare a contact list of all equipment, supply, software, etc., vendors that will provide key services and products to the alternate facility. Integrate this information into the overall notification section of the plan.

Location of the alternate site may require special transportation arrangements. Provisions need to be made for transportion to the alternate center. Include gathering points, identification of charter bus or plane services, arrangements for tickets, travel expenses, per diem, etc.

If business function personnel are forced to work in locations far from home, arrangements for food and shelter must be made for personnel when not working. Planners need to ensure the availability of accommodations to house workers in close proximity to the alternate site. Food service companies or caterers may need to be identified in advance. Restaurants in the vicinity of the site should be identified and their locations designated on a map for distribution to personnel when arriving. Expenses such as these should be met by the organization. When selecting a strategy, expenses incurred over time for prearranged resources should be compared to costs of acquiring resources at the time of the event. Unavailability, delays in delivery, installation, testing, and logistical problems may add more to the costs than can be anticipated.

Determining the appropriate expenditure for a selected strategy includes the cost of the elements that must be restored to working order, the nature and cost of the standby resources dictated by the amount of time recovery can be delayed, and the cost of the combination of resources to sustain the recovery effort.

Hotter business function recovery strategies are available through various vendors' mobile recovery capabilities or business recovery facilities at a fee structure similar to hot site contracts: subscriptions, declaration fees, and daily usage fees.

Texas agencies and universities have legislated mandates concerning the selection and use of disaster recovery-related services. Before beginning any procurement procedures for these types of services, agencies should review Article IX, Sec. 9-6.23, of the General Appropriations Act (76th Legislature) for information about the West Texas Disaster Recovery and Operations Data Center.

Types of Business Recovery Strategies

Midrange Systems. The criticalness of midrange systems is often underestimated. These systems share the same list of potential recovery strategies as mainframes. Shippable and transportable recovery alternatives may be feasible. Cold site and repair or replacement recovery time frames can be much shorter for midrange systems (e.g., days instead of weeks), because many systems do not require extensive facility conditioning. Recovery at the time of disaster often requires people with extensive skills in networking, environmental conditioning, and systems support. Midrange systems are notoriously slow in restoring data.

Business Function Systems. Numerous commercially available products are becoming available for work group recovery. The goal is to re-establish essential day-to-day business functions before consequential effects occur. Most organizations find it necessary to move their employees to an alternate location or to relocate the work itself.

Desktop Computers and LANs. Planning is difficult because of the absence of standardized backup devices that are not always downward compatible. It is difficult to acquire older, compatible technology at the time of a disaster. Use of commercial, shippable microcomputers or LAN capabilities is becoming more common.

Client Server. These customized machine configurations are frequently not stocked in quantity by local computer suppliers, and replacement can be quite difficult. *Internal* reciprocal and redundant options are being used for the file servers. One network software company and some recovery vendors are making file servers available as a shippable alternative.

LANs/WANs. Technological obsolescence must be considered in any long-term LAN recovery strategy. Reciprocal agreements require that hardware remain compatible over time. An even more difficult planning consideration is special network wiring facilities, making relocation difficult. In the absence of these facilities or in a regional disaster, shippable microcomputers that include installed network capabilities are the safest alternative. Lack of industry standard communications hardware is a problem in local and wide area network recovery, making rapid replacement at the time of the disaster risky. Several shippable products (bridges and gateways) are commercially available. If not available, stockpiling of redundant equipment is usually the only recourse. Business recovery for WANs is still in its infancy. It is primarily a network planning issue.

Network Recovery. Network recovery strategies should address all technology and facilities required to reestablish connectivity. This includes person-to-person, person-to-computer, and computer-to-computer connections. The same recovery strategies previously described for computer and work group recovery can be applied to all network components.

Business Function Recovery Facility. Loss of a business function facility requires replacing all equivalent network components. These components include telephones, terminals, control units, modems, LAN network wiring, and the PBX. They may be already in place in an existing redundant, reciprocal, or commercial hot site or cold site facility. The same set of planning issues and network business recovery strategies can be employed.

Access to Communications. A disaster may affect the communications infrastructure outside the facility. Two possible recovery strategies can be used: relocating to an alternate facility in which the infrastructure is in place, or reconnecting to the surviving infrastructure through alternative facilities.

Electronic Vaulting. This emerging business recovery strategy can decrease loss of data and shorten recovery windows. Commercial disaster recovery vendors provide both remote transaction journaling and data base shadowing services. Costs for electronic vaulting are expected to decline. The business impact analysis process helps determine when this strategy is justified.

Comparing Strategies

The following table is an example of how to provide a comparison of various types of strategies based on recovery time frames, advantages, and disadvantages.

Reciprocal agreements sound better in theory than in reality. Historically, these types of agreements are seldom reliable and often fail when they are needed.

Strategy	Recovery Time Frames	Advantages	Disadvantages
Repair or rebuild at time of disaster	6-12 mo.	Least cost	Time to recovery, reliability, and testability
Cold Site (private or commercial)	1-6 weeks	Cost-effective / Time to recover	Testability, detail plans are difficult to maintain, long-term maintenance costs
Reciprocal Agreement	1-3 days	Specialized equipment in low-volume applications	Maintenance and testability
Service Bureau	1-3 days	For contingency planning (e.g., backup microfilm)	Not available in large CPU environments
Shippable or transportable equipment	1-3 days	Useful for midrange computing	Logistical difficulties in regional disaster recovery
Commercial Hot Site	Less than 1 day	Testability / Availability of skilled personnel	Regional disaster risk
Redundant facility	Less than 1 day	Greatest reliability	Most expensive, long-term commitment and integrity

Definition

A recovery plan is a manual with procedures, responsibilities, and critical information needed to execute a recovery. Recovery from the loss of facilities, information resources, and skilled key personnel is generally the accepted approach to building a recovery plan. A fundamental premise of a successful business continuity plan is that the plan is developed by those who must actually carry out the recovery in the event of an actual disaster.

The planning effort should be centrally coordinated to ensure that the recovery plan

- Is commensurate in scope with the impact and magnitude of loss or harm that could result from an interruption;
- Identifies and ranks subsets of critical and essential business function activities and processes based on how long the organization can survive without each one;
- Reduces confusion during a chaotic period by documenting an orderly recovery process that ramps up recovery at an acceptable, although degraded level, reducing impacts to the organization over an extended period of time;
- Identifies minimum recovery resources and establishes a source for each;
- Develops or uses available and/or cost effective recovery strategies;
- Contains written, step-by-step procedures and documentation that addresses all elements of the plan;
- Provides an annual testing and maintenance process to ensure accuracy and currency of the plan.

Recovery of end users, networks, and distributed systems was given little attention in traditional disaster recovery planning. The proliferation of departmental computing, desktop workstations, and local area networks has led to a more complex problem than the traditional planning (recovery of a central mainframe computing center). An ever increasing volume of mission-critical data resides in user work areas. The user work areas are more likely to be a site of a disaster than are data centers with their secure, environmentally controlled, routinely backed up, and power-protected systems.

With management approval of the analysis findings and strategy recommendations, the plan is developed by documenting the steps to implement the strategies following an event. The plan must be a carefully crafted report of strategies, broken into tasks and procedures, and an emergency decision-making flowchart.

Since the plan must remain current to be effective, it should be designed with ease of use and maintenance in mind.

The Planning Goal

An agency's goal should be for all its critical business functions to have fully documented and tested disaster recovery plans. This goal offers the ability to

- Understand inter-business work flows;
- Assess the impact of any business disruption or other loss;
- Identify all mandated agency functions;
- Establish the priority and sequences of recovery;
- Take stock of work in progress and evaluate data synchronization for recovery;
- Document all skills, inventories, software needs, and manual procedures necessary for recovery;
- Establish risk control programs based on analyses of personnel resources and environmental risks; and
- Support training for new employees and cross-training for present staff.

Elements of a Recovery Plan

The plan must include everything that end users need to meet their work requirements. They must have a location from which to work that provides comfortable surroundings where useful work can be performed, although it does not have to be as spacious or well appointed as the home site. The location must be equipped with what ever resources are required to perform the critical function, i.e., supplies, office machinery, furnishings, mail, etc.

It is important to understand that for most functions, fewer staff is required in recovery than in normal situations.

Each department manager must identify which personnel are needed to perform the critical processes. Some processes can be postponed until later. Some personnel may be told to go home or could be reassigned or retrained to temporarily perform another more critical function until things return to normal. Assigned personnel must be familiar with the processes and workflow of the function.

Each work group or process being recovered requires representatives with managerial and technical skills. These personnel are responsible for assisting in the preparation of the new work area following a disaster. They also participate in the maintenance of the disaster recovery plan as it pertains to their managerial or technical role.

Users provide the knowledge and skill to accomplish the business function performed by the unit. The work of these personnel comprises the actual recovery of the business function. Customers will deal with these personnel, systems will be used by them, and networks will be connected for their access needs. Users are the primary resource of:

- Recovery information used to develop recovery procedures,
- Resource allocations,
- Scheduling, and
- System and network configurations.

System recovery must be accomplished in the plan for users to access system resources and mission-critical applications. The acquisition and installation of end-user terminals or workstations must be part of this plan and is a technical responsibility.

Network recovery is often overlooked, yet users must have access to voice and data communications capabilities to do work with recovered systems. Network recovery is made easier if the location of the user recovery center is known in advance for implementation of network rerouting strategies.

Recovery Plan: Items to Consider

Important items to address in the plan are provided on the next few pages. The business function recovery and resumption parts are at a task level to better define the details associated with business function recovery.

A variety of example checklists are also included in the appendices.

A wide range of items to consider as a framework when preparing a recovery plan are contained in the following list. Responsibility by an individual or group for each item depends entirely on the size and complexity of the organization. All of the items should be seriously considered for possible inclusion in a recovery plan and be as extensive as the needs of the organization dictate.

Policy Statement

Example: Business function managers and personnel are responsible for formulating, testing, and maintaining recovery plans for their critical services and processes.

Scope Statement

Example: The scope of this plan is to restore critical business functions and systems within __ hours, and essential business functions and systems within __ week(s) of a disaster.

Plan Objectives

Example: To ensure the safety and well being of people, delegate authority to respond, recover critical business functions and support entities, minimize damage and loss, resume critical functions at an alternate location, and return to normal operations when possible.

Roles and Responsibilities—for plan development, maintenance, testing, and implementation

The following components of the planning process and plan development should be completed with detailed steps that include

- authority,
- responsibility,
- procedures,
- tasks, and
- action steps

for each administrative, support, business function, and information resources unit of the organization. Teams have responsibilities with plan development, maintenance, testing, and implementation of the recovery plan.

Incident Response Procedures

- Emergency response (the who and how to report, evacuate, respond, notify)
- Problem escalation management and alert levels (the steps taken to solve a problem before it reaches alert levels and the point where disaster declaration must occur)
- Incident management and control structure
- Management succession and emergency delegated-down decision-making authority based on the need for quick decisive action and knowledge of the critical business functions
- Preliminary damage assessment and salvage (to decide whether to stay at the home site and repair and replace or move to an alternate site)
- Declaration and plan activation authority
- Public information dissemination to interface with external groups (e.g., Other state and federal agencies, public, legislature, emergency service organizations, utilities, and the media)

- Comprehensive damage assessment and salvage operations
- Communications procedures (to ensure that the command structure has the information it needs to evaluate the situation and make accurate decisions on how to best respond)
- Status reporting to incident management and control structure

Support Function Procedures

- Building management and facility support for moves to alternate sites and repair and restoration of home site
- Finance, procurement, travel, per diem, etc.
- Human resources and personnel tracking
- Voice and data telecommunications
- Telephone forwarding, recorded messages
- Telecommuting
- Vital records retrieval and management
- Legal council
- Public information
- U.S. mail and delivery service rerouting
- Food service
- Recovery resource acquisition
- Storage retrieval

Business Function Planning Tasks

- Conduct planning orientation meetings (introduce the planning team, review planning process, recovery approach and expected results, qualifications and roles of participants)
- Review deliverables (business impact analysis, recovery assumptions, coping strategies, command and control strategies, data collection process, meetings and reports)
- Review required resources (personnel, time, data, level of responsiveness)
- Perform business impact analysis
- Document business functions at a task level and required resource dependencies by performing a business process study (see example in Appendix 1)
- Review and establish recovery strategy

- Develop detailed command and control, response, recovery, and restoration procedures
- Establish testing strategy
- Establish maintenance strategy
- Develop training and orientation program

Business Function Recovery Tasks

- Call support services to report disaster
- If long-term outage, send non-critical and non-essential staff home
- Receive details of disaster if not present
- Review public announcement policy
- Initiate telephone and fax notifications and log accordingly
- Call business function recovery team members
- Notify staff members
- Give location of meeting place and times to report, if appropriate
- Aid in damage assessment if required
- Salvage vital records and equipment
- Initiate progress log
- Establish temporary location
- Confirm temporary facility requirements
- Obtain location of temporary facility
- Notify employees of alternate site
- Verify security at alternate site
- Post signs at work locations
- Retrieve off-site materials needed to perform work
- Verify that all off-site materials were received
- Inform coordinator if material is missing
- Ensure that telephone service is restored
- Determine number of available personnel
- Inform clients, agencies, etc., of new location
- Inform vendors of new business location
- Determine office supply packet requirements
- Review minimum office requirements

- Place order for rubber stamps if needed
- Confirm general forms requirements
- Confirm special forms requirements
- Review necessary personal computers and software
- Review critical, external data communications
- Prepare for arrival of furniture
- Order necessary external documentation
- Review special equipment requirements
- Communicate status to business recovery coordinator
- Breakdown and describe all tasks to be recovered
- Organize work force and begin startup
- Use manual procedures to resume business
- Begin deferred transaction recovery procedures
- Begin lost transaction recovery/catch-up procedures
- Report status to business recovery coordinator
- Critical automated reports
- Establish data processing connections
- Establish PC capability
- Establish other vendor connectivity
- Verify that restored PC files are correct
- Verify that proper on lines are restored
- Complete lost transaction recovery process
- Meet with your personnel to evaluate status
- Report status to business recovery coordinator
- Begin business operations

Return to Home Site Tasks

- Meet facilities preparation team to plan move
- Set move date
- Establish equipment needs
- Establish special equipment or furniture needs
- Establish CRT, PC, and printer needs

- Establish telephone needs
- Establish security needs during move
- Start up business processing
- Forward status to business recovery coordinator

Recovery Plan Attachments, Activity Reports, and Logs

- Recovery phase time line
- Telecommunications resources
- Floor plans of home and alternate sites
- Office space considerations
- Location of drops, phone lines, activation
- Recovery configuration schematic
- Recovery time line report
- Personnel notification list, log
- Team composition list
- Recovery time line, log
- Vital records list, log
- Customer contacts list, log
- Inter-agency support list
- Vendors and suppliers list, log
- Recovery configuration list
- Physical and logical security requirements
- Capitalized inventory list
- Repair and restoration log
- Damage assessment log
- Plan distribution list

Justification

The analysis and plan development stages of the recovery effort is only the beginning. Testing and maintenance is an ongoing program of validation and updating the documentation. Testing does not create pass/fail situations. Tests (sometimes called exercises) expose the areas in the plan that need to be revisited.

If an exercise has perfect results, worry.

To help senior management understand the importance of testing, proper communication of the risk involved in not having an adequate testing program is necessary. The best approach is to frame the discussion in terms of risk avoidance. An organization's failure to act can be a critical point in claims against it. Recovery plan testing demonstrates the safeguarding actions taken prior to an event. Testing proves the recovery plan will work and how it can be improved, thereby raising the overall probability of a successful recovery or reducing the time to complete recovery.

An interim move back to manual procedures for a testable recovery strategy is seldom a feasible option anymore because of the extent to which automated procedures have replaced manual procedures in the business process. With the recent trends in downsizing, the resources to move back to a manual processing mode for an interim period often do not exist. Therefore, the need to maintain the agency-mandated functions must be articulated as part of the basic vision of the testing efforts.

Often, the staff simply does not exist in sufficient numbers or the staff that is present is unlikely to be familiar with the manual process formerly in place).

Testing must concentrate on high priority applications and business functions that were determined during the impact analysis. The identified losses help to justify testing because the cost of doing nothing (i.e., the cost of failure) has been determined. Also, the business impact analysis determines the recovery window, which then helps determine the appropriate strategy. It is the plan and the strategy that is being tested.

Similar to any other product, the business continuity plan must be tested before it is deemed usable or dependable enough to enable the organization to perform the critical

function with alternate resources. Each time the system is updated or changed, the plan must be exercised for effectiveness. Maintenance of the business continuity plan, like any system or application, should be included in the budget as a line item in the methodology process.

Testing Objectives

Testing objectives should be set to start small and increase in complexity and scope over time. Achieving the following objectives provides progressive levels of assurance and confidence in the plan. An attainable and clearly stated testing program should

- Not jeopardize normal operations;
- Increase, over time, the complexity, level of participation, intent of the activity, functions, and physical locations involved;
- Demonstrate a variety of management and response proficiencies, under simulated crisis conditions, progressively involving more resources and participants;
- Uncover inadequacies so that configurations and procedures can be corrected; and
- Meet the end users' requirements for recovery based on a thorough understanding of customer specifications and the resultant deliverable—an effective recovery plan.

Test/Exercise Types

Test types vary from minimum preparation and resources to the most complex. Each bears its own characteristics, objectives, and benefits.

Orientation/Walkthrough. Activities are characterized by

- Execution in a conference room or small group setting;
- Knowledge, rather that skill validation;
- Individual and team training;
- Critical plan elements are clarified and highlighted;
- Team-building focus by individual management/response groups;
- Interactive discussions among participants;
- Response and management dialogue guided by moderator;
- Documentation of participant discussions;
- No mobilization of resources;
- No simulation except as necessary to prompt consideration of pertinent issues;
- Assessment of participant knowledge relative to training objectives.

Tabletop/Mini-drill. Activities are characterized by

- Practice and validation of a specific functional response capability;
- Focus on demonstration of knowledge and skills as well as team element interaction and decision-making capability;
- Actual role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening format;
- Mobilization by limited elements of the crisis management/response organization to practice proper coordination;
- Varying degrees of actual, as opposed to simulated, notification and recourse mobilization to reinforce the content and logic of the plan;
- Simulation of nonparticipating, essential activities that impact response efforts;
- Use of controllers to ensure that activity remains within intended scope of the exercise;
- Evaluation of performance and ability of multiple elements to work together effectively, demonstrate specific skills, decision-making abilities, and knowledge of response operations relative to drill objectives.

Functional Exercises. Activities are characterized by

- Demonstration of emergency management capabilities of several groups practicing a series of interactive functions such as direction, control, assessment, operations, and planning;
- Actual or simulated response to alternate locations/facilities using actual communications capabilities;
- Involvement of multiple emergency organizations and various organizational units of the organization, with optional involvement of external groups (fire department, EMS, etc.);
- Mobilization of personnel and resources at varied geographical sites;
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization;
- Simulation of nonparticipating, essential activities that impact response efforts;
- Use of controllers, evaluators, and observers to ensure that activity remains within intended parameters of the exercise;
- Evaluation of individual/team performance relative to exercise objectives;
- Introduction of realistic and unexpected complication(s) in the exercise scenario (optional).

Full-scale Exercise. Activities are characterized by

- Validation of crisis response functions;
- Demonstration of knowledge and skills, as well as management response element interaction and decision-making capability;
- Most complexity, as it generally involves elements which are outside of the span of control of a single entity;
- On-the-scene coordination and policy-making roles are demanded;
- Direction and control, mobilization of resources, communication, and other special functions are rigorously exercised;
- Actual response locations/facilities;
- Involvement and interaction of all internal and external management response elements with full involvement of external organizations;
- Exercises generally extend over a longer period of time to allow issues to fully evolve as they would in a crisis, and allow realistic play of all the involved groups;
- Mobilization of all combined elements of the crisis management response organization;
- Actual, as opposed to simulated, notification and resource mobilization;
- Use of controllers to ensure that activity remains within intended scope of the exercise;
- Evaluation of collective company performance relative to the exercise objectives.

Conducting the Exercise

Testing requires some centralized coordination, usually by the recovery planning coordinator, because of his/her contingency planning knowledge and understanding of how the business continuity team plan interacts with the overall recovery strategy of the organization. The coordinator is also responsible for overseeing the accomplishment of targeted objectives and follow-up with the appropriate areas on results of the exercise.

Design the testing program to start with the basics and build up with each test becoming more complex and comprehensive than the previous. For example, test the ability to bring up the operating system from the backups stored off-site. Next, bring up the operating system and an application on an alternate processor. Then, test user access and ability to perform transactions. Later, include users from different locations and with different resources dependencies.

Participants should fully use their resourcefulness to overcome the problems within the restraints of the test scenario.

Vary scenarios so all major elements of the plan are validated within a specified period and under various time, weather, and operational conditions.

Example: A critical document was not available where the most accessible copy was known to be in the burning building. In reality the recovery effort would not stop. People would brainstorm where additional copies may be and then try everything possible to obtain a copy.

More personnel participating in the exercises allows greater exposure and more resources familiar with the business recovery plan, which increases awareness, buy-in, and ownership. Try to rotate personnel involvement in annual testing to be prepared for retirements, promotions, terminations, and/or transferring of tasks. All team members need multiple exposures to the procedures they are to follow under a variety of conditions. Some tests can be unannounced—but none should be infrequent. Long periods of inactivity can result in a deterioration of skills and understanding of roles and responsibilities. If well managed and supported, testing can serve to validate an organization's crisis management/ response program and ensure continued involvement and improvement.

Mistakes, repetition, and eventual success are strong learning tools.

Tests need to have a strategic combination of the following elements:

- Trials—to assure that component resources come together to produce expected results and that written procedures are in place to bring those resources into play efficiently.
- Training—to assure that personnel assigned specific recovery responsibilities are prepared to carry out the tasks needed to fulfill these responsibilities.
- Exercises—to bring the resources, procedures, and personnel together to make the recovery plan work on an ongoing basis.

Examples of parameters for conducting tests:

- Participants are restricted to material carried in or stored off-site, not by what is dependent on their own memory or knowledge.
- Have procedures for documenting instances when the lack of vital information, a key resource, or an inadequate procedure keeps the team from attaining the testing objective(s). This type information is used to evaluate the test and update the plan.

Testing is NOT business as usual! Personnel and resources made available are for completion of identified testing scenario and its critical tasks only.

Evaluate the Exercise

A successful exercise is *one that reveals problems*. Therefore, a less-than-successful exercise, one where no problems were noted and everything seemed to work like clockwork, could foretell less-than-successful crisis response capability in a real situation. It may also mean the test was poorly designed.

Evaluation should occur within one to three weeks of the exercise. Participant evaluation by the business recovery team is an option as well as outside entity evaluation, such as internal audit personnel.

The exercise critique reviews performance, documents lessons learned, assesses capabilities of personnel and adequacy of dedicated equipment, and identifies deficiencies in the crisis management plan.

An evaluation process, with input from the participants and evaluators, includes the following:

- Different points of view and observations about problems that occurred.
- Instances of resourcefulness used to overcome the problems within the restraints of the scenario.
- Written records of deficiencies and corrective actions.
- Unrealistic or undocumented assumptions, especially with respect to staffing.

Examples of undocumented assumptions within the disaster may include:

- All personnel are unaffected by the disaster event and available for recovery duty.
- No key person is traveling or on vacation.
- All personnel can move freely to the recovery location with no impediments to travel.
- All individuals are available for the length of time that may be required for recovery.
- All personnel are concentrating on completing disaster recovery for the organization and not be distracted by personal concerns.

Recommendations include provisions for additional training, assignment of appropriate personnel, suitability and performance of equipment, and changes in scope or thoroughness of the plan.

Management reports are prepared following the evaluation. Management needs to know:

- If the objectives of the test were completed,
- Where short-falls exist, and
- The recommendations for the next testing period.

The business function manager and the business recovery coordinator should use the evaluation for planning subsequent tests and exercises.

Update the Plan

Although test evaluations are important in refining the plan, other factors within the organization can also contribute to the need for plan updates. The plan is an ongoing maintenance process and may not wait for the annual exercise.

Examples of changes that affect plan maintenance include, but are not limited to:

- Personnel changes,
- Personnel information changes,
- Functional changes,
- Major changes in IT environment, and/or
- Changes in agency direction.

When the plan is updated, the team and the business recovery coordinator must be informed of changes. Copies are distributed to team personnel and a duplicate copy is secured off-site. Each copy should be secured and labeled "Confidential" due to personal information within the plan, e.g. emergency medical information and home telephone, pager, cellular telephone, and social security numbers.

Many agencies use automated software packages to develop and maintain the plan or standard word processing packages; either are acceptable.

Establish a tentative date for the next exercise. The test cycle ensures that a full year does not elapse between exercises. Here the objectives, as identified previously, should increase dependent on the criticalness of the business resumption plan. A plan not exercised within one year becomes obsolete, resulting in a waste of the previous efforts dedicated to the creation and success of the recovery plan.

Some Final Thoughts

Successful continuity plans that produce desired results under comprehensive and realistic tests, including real outages, are the ones structured from the *business side* rather than technology or a specific process. Plans are successful when

- The approach to continuity planning is a part of agency planning.
- Plans are the results of cooperative thinking and are designed by a cross section of involved and responsible management and key personnel rather than a few specialists.
- Plans are based on completed and realistic business impact analyses that are revisited to ensure continued viability as business scope and processes change.
- BCPs are regarded as a business characteristic equal in importance to speed, accuracy, capacity, flexibility, ease of use, safety and security, and integrity.
- The plan can contribute to the overall quality, productivity, and success of the organization, not just an overhead exercise.
- Plans are tested realistically and with appropriate stress.
- There is follow-up and action on test results.
- Plans are updated as a normal course of operations when changes in business, organization, staffing, processes, and technology require them.
- Consideration is given to looking for the cost-effective prevention as well as reactive measures.
- Plans are given high priority and follow-through is energetic on planning and decisions.

While a total overview of the BCP process has been presented, please be aware that actual planning and implementation can be phased in order to stay within practical resource and timing constraints. It is always better to have an effective plan for one site than to be in the midst of planning for the "world" and not survive a single-site disaster. Ensuring that the highest risk locations are ready to respond and recover first is always an effective approach.

The Bottom Line: Continuity planning is a business process requiring business management attention and guidance.

Continuity planning is a learning experience about the agency. It is not an event, it is an ongoing process. It should become an integrated part of business management. Significant changes trigger consideration of the continuity consequences.

Appendices

Important Note:

All agencies and universities have unique missions and environments. The appropriateness of generic checklists should always be a consideration for each environment. Checklists are a tool to help keep track. Recovery personnel MUST NOT rely solely on them. Remember that customization will be required to match agency requirements.

Business Process Study for Business Operation: Open Records Request

The purpose of this study is to modify standard operating procedures (SOPS) for use during recovery conditions in the business function recovery plan. The study reduces normal business operations to a level that can be performed with only minimum resources during extreme conditions. It also identifies the inputs required to perform the function and the outputs that must occur for other critical business functions to begin work. Perform the following business process study for all critical functions, include inputs, outputs, resource or service dependencies, etc. Open Records is used as an example only.

For each business operation/function, perform the following:

1. Itemize normal processes.
2. Identify what resource is required.
3. Modify normal processes to short cuts (i.e., approvals, record keeping, filing, anything than can be skipped or delayed)
4. Modify the resources required.
5. Explain in comments.

	1. Normal SOPs	2. Normal Resources	3. Modified SOPs	4. Modified Resources	5. Comments
DAY 3	1. Calculate deadline 2. Contact requestor 3. Request requirements (programming, manipulation of data)	JOB FUNCTIONS: • Open Records Liaison • Open Records Attorney • Legal Assistant	• Receive mail, separate Open Records Requests • Record Requestor Name • Mail form Letter or telephone requestor • List of alternate sources of information	• Incoming Mail • 1-2 staff persons • Telephone • Form Letter • Copier • Outgoing Mail	Government entities have 10 days to notify the requestor that the information cannot be provided in 10 days.

	1. Normal SOPs	2. Normal Resources	3. Modified SOPs	4. Modified Resources	5. Comments
DAY 3	4. Copy to appropriate persons: Who? • send copy • coordinate • copy ISD • copy to Legal Dept. 5. Check Clearly Public list 6. Consult attorney non-public	INPUTS: US Mail, Telephone, Internet, Web Page EXTERNAL DEPENDENCY: OAG OUTPUTS:	Record message on 1-800 number, TV and radio, PIO.		
	1. Can produce in 10 days? 2. Information accessible? 3. Requestor need copy 4. Calculate charges 5. Mail copies, provide access	INFORMATION RESOURCES: MEDIA: HARDCOPY FILES: ACCESS TO EXTERNAL DATABASES:			
	1. Forward processing request to IS 2. IS will analyze request 3. Provide information to requestor 4. Notify requestor regarding availability of requested information				

By completing these steps, you have basically written the procedures that will be followed during a disaster, identified the minimum resources required to perform them, which is the basis of each functional or operational area's business recovery plan.

APPENDIX 2

Business Impact Analysis

This questionnaire is meant to assist the business process owner or the application owner in assessing the risk or organizational impact of the loss of the business process and its associated applications. If, at any point, the process is determined NOT to be vital, it is not necessary to complete the questionnaire.

Business Process: _____

Dependent Processes (Input and Output): _____

_____

_____

_____

(Use reverse side if additional space is needed)

1. The loss of this business process would have the following effect on the organization:
   _____ A. Catastrophic effect on the organization or some divisions
   _____ B. Catastrophic effect on one division
   _____ C. Moderate effect on the organization
   _____ D. Moderate effect on some divisions
   _____ E. Minor effect on the organization or some divisions

2. How long can your business process continue to function without its usual information systems (IS) support? Assume that loss of IS support occurs during your busiest, or peak, period. Check one only.
   _____ Hours
   _____ Up to 1 day _____ Up to 2 days
   _____ Up to 3 days _____ Up to 1 month
   _____ Up to 1 week _____ Other (please specify)_____

   Indicate the peak time(s) of year and/or a peak day(s) of the week and/or peak or most critical time of the day, if any, for this business process or its associated applications.

(Month)	J	F	M	A	M	J	J	A	S	0	N	D
(Day)	S	M	T	W	T	F	S					
(Hour)	0	1	2	3	4	5	6	7	8	9	10	11
	12	13	14	15	16	17	18	19	20	21	22	23

Contributing information to this example comes from Eastman Kodak Company and Texaco, Inc.
Any use or reproduction of this example should include this statement of credits

3. Are there any other peak load or stress considerations? _____
   _____
   _____

4. Have you developed/established any backup procedures (manual or otherwise) to be used to continue business processing in the event that the associated applications are not available?_____
   _____
   _____
   _____

   If yes, have those procedures been tested? IS only? Non-IS?

   Did the test including business process functional users?
   _____ Yes, within the past 6 months
   _____ Yes, within the past year
   _____ Yes, but over a year ago When? _____
   _____ No

Use the following alphabetical codes to answer questions 5, 6, and 7:

A = Over $1OM	B = $1–$1OM	C = $1OOK–$1M	D = $10K–$100K	E = Up to $10K

5. The loss of this business procedure would result in lost revenue from fees, collections, interest, penalties, etc. During the indicated time after the disaster, this loss would be:
   _____ Hours___ _____ Day 2 _____ Week 1 Other
   _____ Day 1 _____ Day 4 _____ Month 1 _____

6. The loss of this business process would erode our customer base over a period of time. The cost to the organization from lost business, after the time indicated, would be:
   _____ Hours___ _____ Day 2 _____ Week 1 Other
   _____ Day 1 _____ Day 4 _____ Month 1 _____

7. The loss of this business process would result in fines and penalties due to regulatory requirements (federal, state, local, etc.). The total of these Fees, after the time indicated, would be:
   _____ Hours___ _____ Day 2 _____ Week 1 Other
   _____ Day 1 _____ Day 4 _____ Month 1 _____

8. The loss of this business process would have the following legal ramifications due to regulatory statutes, stockholder requirements, or contractual agreements: (Specify the area of exposure) _____
_____
_____

9. The loss of this business process would have the following negative impact on personnel in this organization: _____
_____
_____

10. The loss of this business process would keep us from supplying the following services to outside customers: _____
_____
_____
_____

11. Specify any other factors that should be considered when evaluating the impact of the loss of this business process: _____
_____
_____

12. Are there ANY other dependencies (staff, vendor, software, unique resources, etc.) not already identified above? _____
_____
_____
_____

13. Does an analysis of the responses to the above questions indicate that this business process should be considered as "vital" to the organization? If yes, indicate below when such a label is appropriate:
    ___ Always
    ___ During the following period of the year: _____
    ___ During the following time of the month: _____
    ___ During the following time of the week: _____
    ___ Other time period. Specify: _____

    Business Process Contact: _____

Contributing information to this example comes from Eastman Kodak Company and Texaco, Inc.
Any use or reproduction of this example should include this statement of credits

Contributing information to this example comes from Eastman Kodak Company and Texaco, Inc.
Any use or reproduction of this example should include this statement of credits

Business Continuity Planning Process Flow

Step 1. Project Initiation

- Identify Customer and Business Requirements
- Identify External Requirements: Government, Industry, and Legal
- Perform Risk Assessment
- Obtain Management Support
- Implement Project Planning and Control Process

Step 2. Business Impact Analysis

- Define Criticality Criteria
- Identify Vital Business Processes, Applications, Data, Equipment, etc.
- Determine Disaster Cost Impact on Business Processes
- Identify Interdependencies
- Define Recovery Time Objectives

Step 3. Recovery Strategies

- Identify Process and Processing Alternatives & Offsite Data Backup Alternatives
- Identify Communications Backup Alternatives
- Identify Recovery Strategy Alternatives (Replace, Outsource, Manual, Etc.)
- Formulate Strategy Based on Optimum Cost-Benefit & Risk
- Review strategy with Recovery Teams, Management and Customers

Contributing information to this example comes from Eastman Kodak Company and Texaco, Inc.

Step 4. Plan Development

- Define Disaster Recovery Teams, Authority, Roles and Responsibilities
- Develop Notification and Plan Activation procedures
- Develop Emergency Response Procedures
- Develop Detailed Recovery Procedures
- Develop Plan Distribution and Control procedures

Step 5. Plan Validation/Testing

- Develop Test Plans and Objectives
- Conduct "Table-top" Simulations
- Perform Tests
- Evaluate Test Results
- Perform Plan Process Improvements Based on Test Results

Step 6. Maintenance and Training

- Develop BCP Maintenance Process
- Consolidate Revision Information
- Develop Revised BCP, as Required
- Develop Corporate Awareness Program
- Develop BCP-Specific Training Program

APPENDIX 4

Distributed System Continuity Plan Components

System

Configuration
Type (NT, AIX, etc.)
Release Level

Network

Type (Ethernet, etc.)
Schematic
Equipment types

Application(s)

Name and acronym
Major Customers
    Department, Contact Name (Emergency, alerts, etc.), Telephone, Pager
Recovery Time Object (RTO)

Backup

Software
Tape device used
Tape type used
Network issues as appropriate
Data Recovery/Replacement Process
Contacts
Expectations
Schedule: on-site and off-site

System and Application

Problem call list (Name, pager, etc.) Primary and alternates
Notification List (Customer, management, etc.)
Escalation procedures

Recovery

Procedural steps for system, application, data, etc.
    Scripts, etc. should be referenced with name & location
Implementation plan
    Minor, Major, Catastrophic
Time to perform major component steps of recovery

Contributing information to this example comes from Eastman Kodak Company and Texaco, Inc.
Any use or reproduction of this example should include this statement of credits

Dependencies (with contact names and numbers)

Other systems
Network
Environmentals
Support teams or individuals
Assumptions that the plan is developed under (power, space, etc.)

Vulnerabilities (with explanation)

Vendor List for hardware, operating system, subsystems, application, etc.

Glossary of Terms

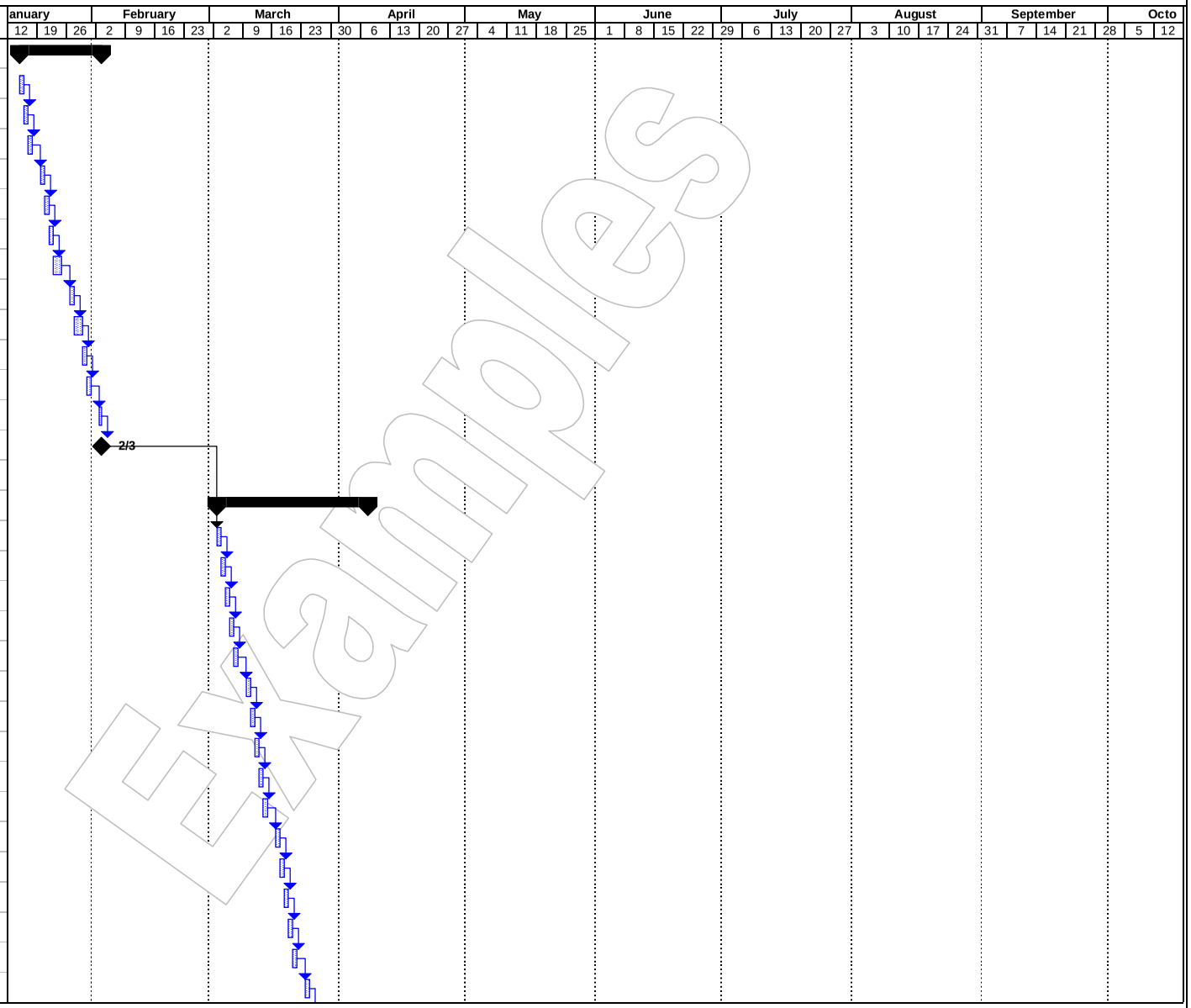
Plan Distribution and Control Procedures

Revision Contact and Process
Distribution List
Change Log

APPENDIX 5

Example of Business Continuity Plan Development Project

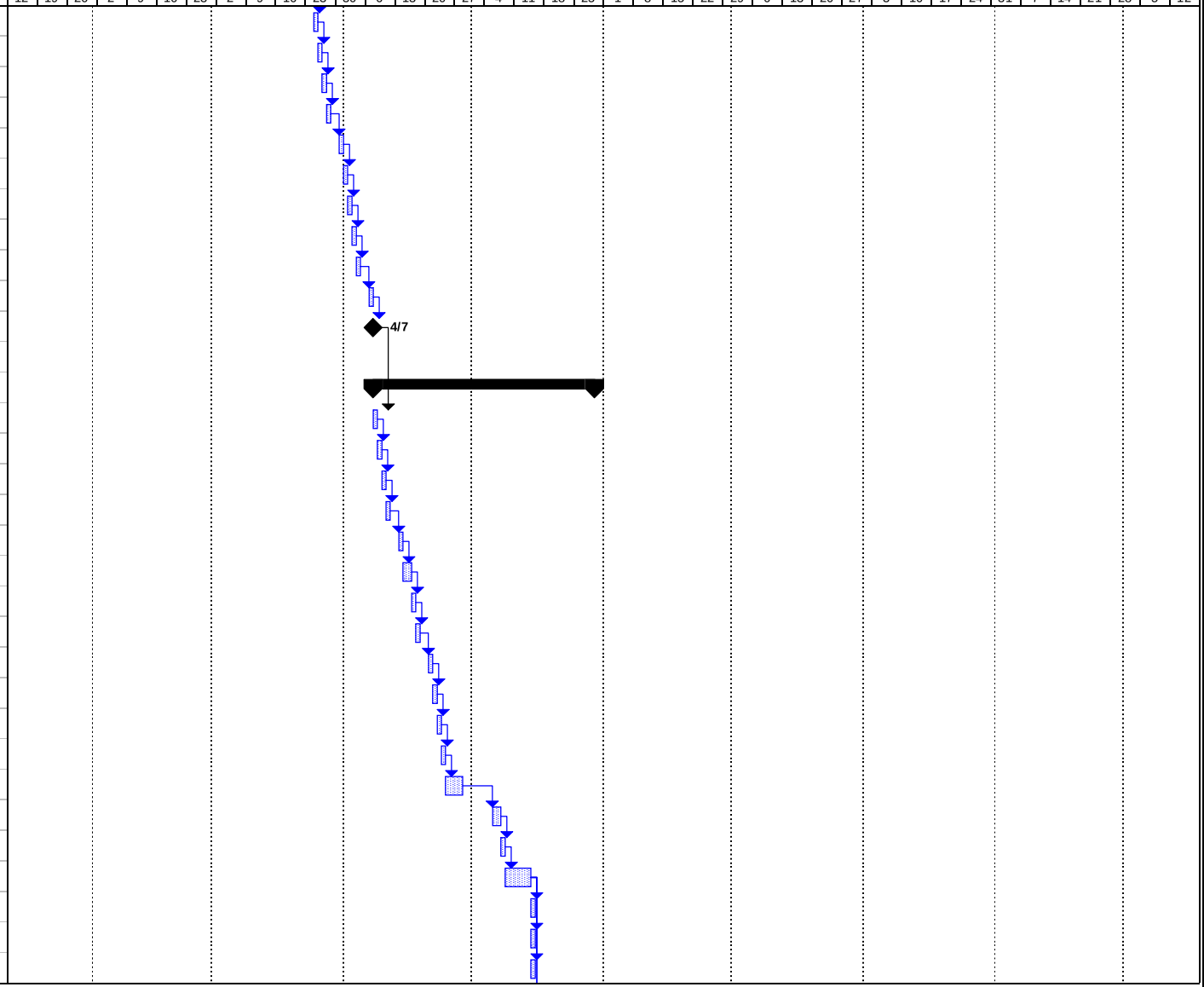
Example of a Business Continuity Plan Development Project



ID	Task Name
1	**PHASE 1--PROJECT INITIATION**
2	Project Kickoff Mtg
3	Project Planning Meeting
4	CLIENT Network Orientation
5	Establish Terms & Assumptions
6	Modify Project Plan
7	Issue Project Specification
8	Conduct Contractual Negotiations
9	Obtain Management Approval
10	Establish Project Team
11	Assign CLIENT People to Project
12	Establish BCP Steering Committee
13	Schedule Follow-on Visits
14	Phase 1 Complete
15	
16	**PHASE 2--RISK ANALYSIS (RA)**
17	Verify Scope & Objectives of RA
18	Develop RA Data Collection Format
19	Conduct BCP Team RA Workshop
20	ID Risks to CLIENT
21	ID Hazards to CLIENT Operations
22	Verify Probabilities of Risks & Hazards
23	ID CLIENT Vulnerabilities to Risks
24	Establish Criteria for Hi/Mod/Lo Vulnerability
25	Categorize Risks & Vuls-Pers/Facil/Fin/Opnl
26	ID Risks with Greatest Impact to CLIENT
27	Verify Vulnerabilities & Categories
28	ID Controls in Place
29	ID Possible Additional Controls
30	Cost Present Controls
31	Cost Additional Controls
32	Analyze Controls vs Risks Avoided

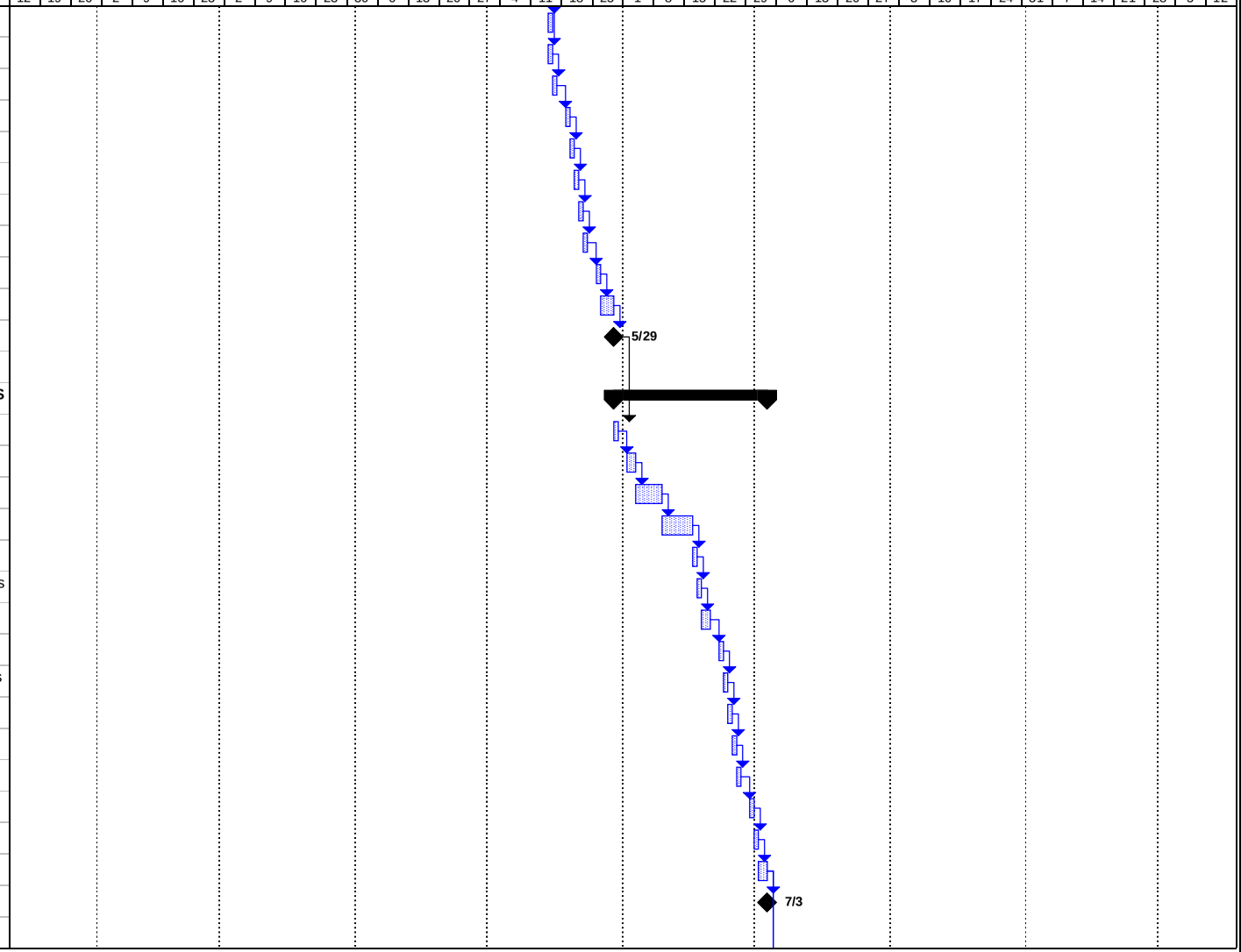
Example of a Business Continuity Plan Development Project

ID	Task Name
33	Establish Probable Risk Scenarios
34	Recommend Addl Controls/Changes
35	Prepare RA Report
36	Prepare RA Presentation
37	Present RA to BCP Teams
38	Present RA to Steering Committee
39	Make Changes Suggested
40	Present RA to Senior Mgmt
41	Make Changes Suggested by Sr Mgmt
42	Deliver Risk Analysis Report
43	Phase 2 Complete
44	
45	**PHASE 3--BUSINESS IMPACT ANALYSIS**
46	Confirm Scope & Objectives of BIA
47	CLIENT Business Orientation
48	Establish Outage Criteria
49	Confirm Threats (Disasters)
50	Conduct BCP Team BIA Workshop
51	Develop BIA Questionnaire
52	ID Questionnaire Recipients
53	Create BIA Professional Diskettes
54	Distribute BIA Questionnaires/Diskettes
55	BCP BIA Teams Complete Questionnaires
56	BIA Info Returned
57	Initial BIA Data Analysis
58	Schedule Interviews
59	Conduct Interviews to Validate Data
60	Summarize Interview Results/Info
61	Compile/Analyze BIA Data
62	Establish Financial Impacts of Outage
63	Establish Operational Impacts of Outage
64	Establish Customer Impacts of Outage



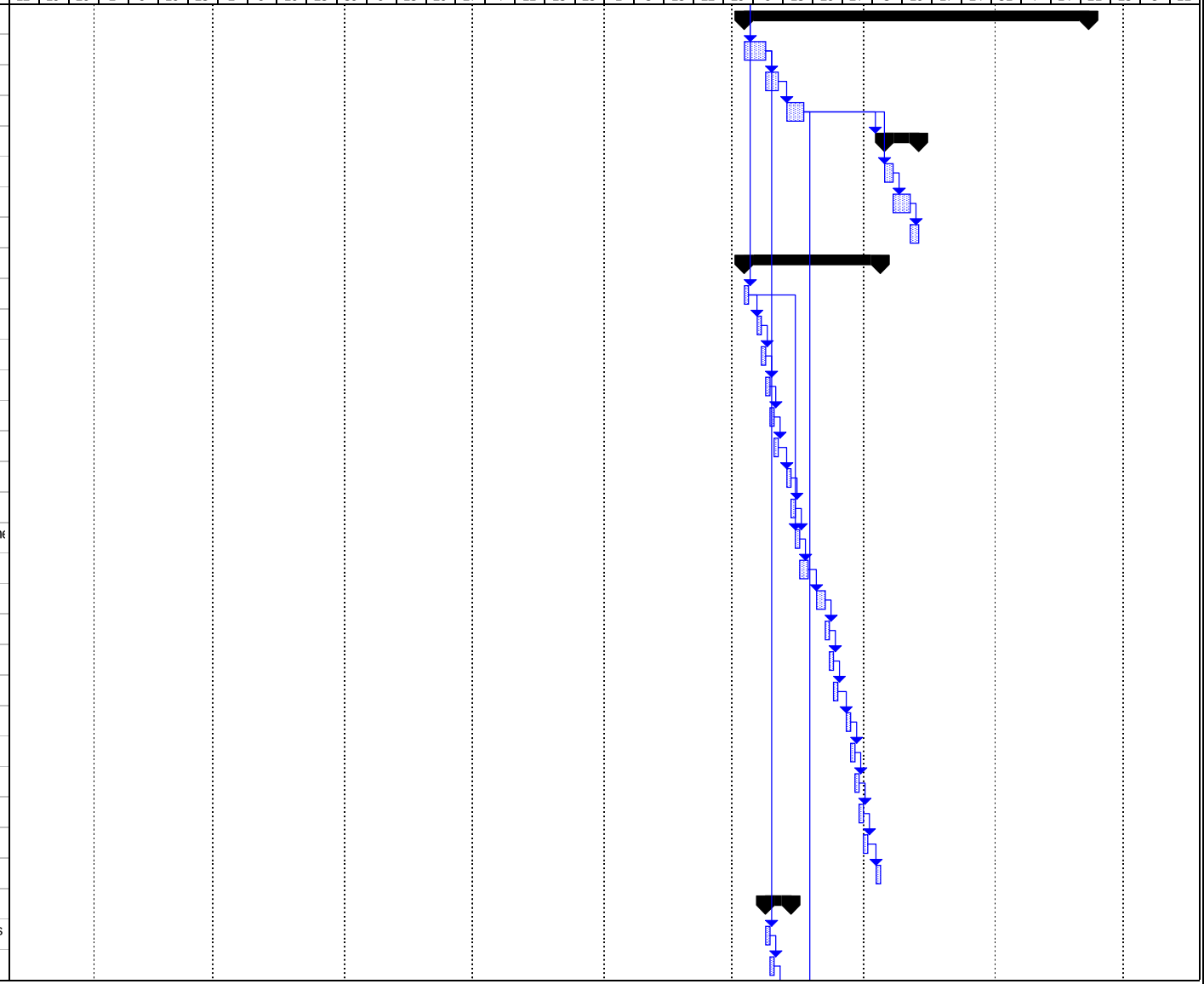
Example of a Business Continuity Plan Development Project

ID	Task Name
65	Establish Legal/Regulatory Impacts of Outage
66	Establish Other Impacts of Outage
67	Determine Recovery Time Objectives
68	Establish Business Unit Recovery Priorities
69	Establish Recovery Requirements/Resources
70	Prepare BIA Report
71	Prepare BIA Presentation
72	Present BIA to BCP Teams
73	Present BIA to Steering Committee
74	Make Changes Suggested
75	Phase 3 Complete
76	
77	**PHASE 4--BUSINESS RECOVERY STRATEGIES**
78	Verify Business Unit Recovery Requirements
79	Define Supporting Technology Requirements
80	ID Recovery Alternatives
81	Establish Costs for Recovery Alternatives
82	Conduct Cost-Benefit Analysis
83	Develop Recommended Recovery Strategy(ies
84	Prepare Strategy Report (BIA Rpt Module)
85	Prepare Strategy Presentation
86	Present Recovery Strategy(ies) to BCP Teams
87	Present Strategy(ies) to Steering Committee
88	Make Changes Suggested
89	Present BIA/Rec Strategy(ies) to Senior Mgmt
90	Make Changes Suggested by Sr Mgmt
91	Deliver BIA/Recovery Strategy(ies) Report
92	Verify Approval for Recovery Strategies
93	Phase 4 Complete
94	



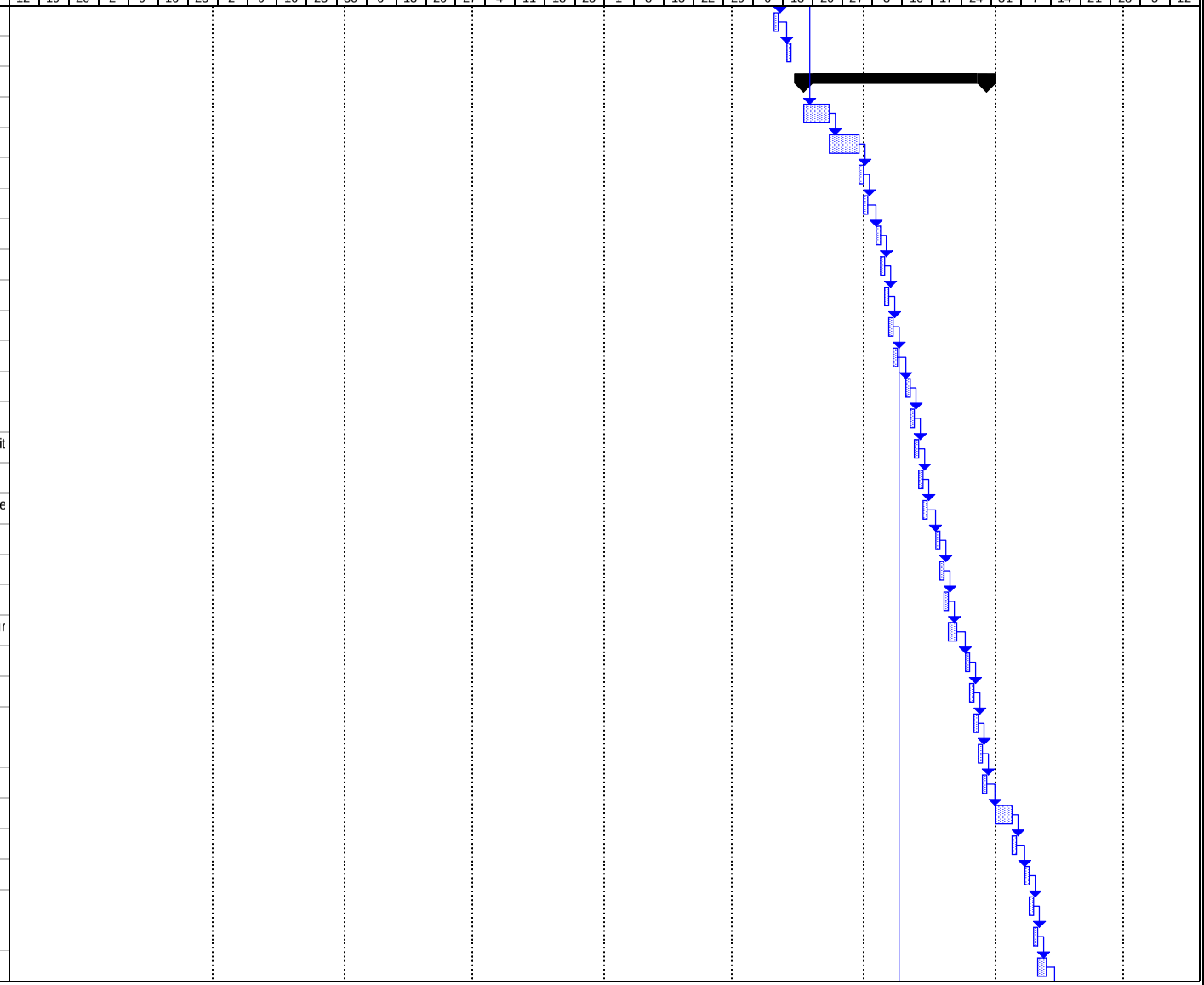
Example of a Business Continuity Plan Development Project

ID	Task Name
95	**PHASE 5--BCP PLAN DEVELOPMENT**
96	Define BCP Organization
97	Define BCP Team Responsibilities
98	Select BCP Team Leaders & Alternates
99	**Verify Business Unit Processes**
100	Conduct Documentation Sessions
101	Capture Dependencies
102	Define Interim Business Processes
103	**Implement Recovery Strategies**
104	Establish Support Contracts
105	Negotiate & Sign Vendor Contracts
106	Install Network Components
107	Purchase Necessary Equipment
108	ID Sources of Temporary Personnel
109	Contract for Addl/Temp Personnel
110	Purchase Hardware
111	Purchase Software
112	Fund Contracts, Sware, Hdware & Equipme
113	Define Normal Inventories
114	Define Recovery Inventories
115	Define Recovery Point Objective
116	Define Data Backup Requirements
117	Define Off Site Storage Requirements
118	Review Records Retention Procedures
119	Plan for Transportation
120	Plan for Supplies
121	Plan for Special Forms
122	Prepare Sites to Support Recovery
123	Verify Advance Preparations Adequate
124	**Link to Emergency Response Plan**
125	Review Emergency Response Procedures
126	Develop Links to BCP



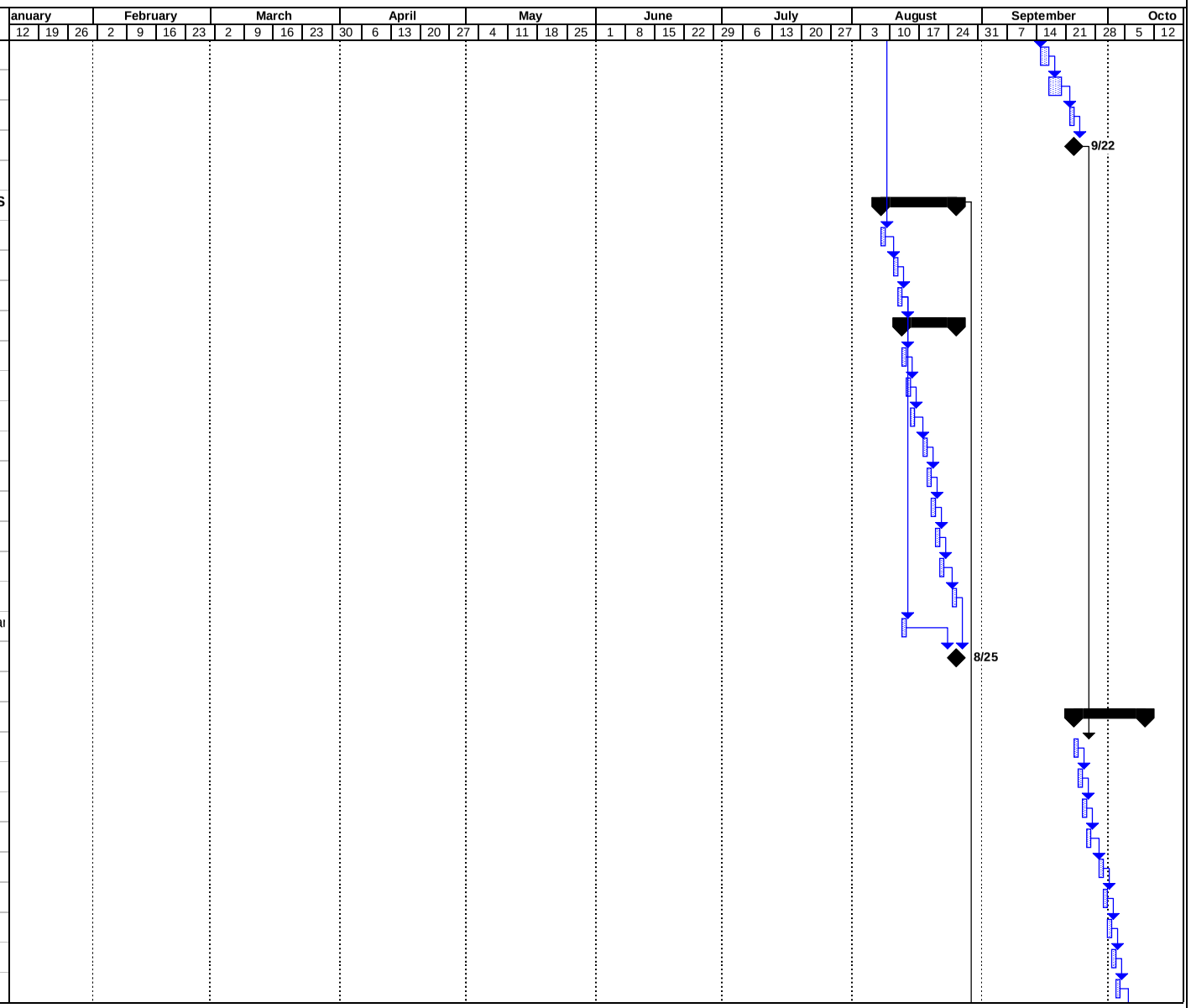
Example of a Business Continuity Plan Development Project

ID	Task Name
127	Ensure Support by Fire/Police
128	Validate with Risk Management & Safety
129	**Develop Team Recovery Procedures**
130	Develop Plan Components (LDRPS)
131	Conduct Training Sessions
132	Establish Phases of Recovery Operations
133	Validate Disaster Criteria
134	Establish Recovery Scenarios
135	Document Recovery Priorities
136	Establish Recovery Times
137	Document Recovery Requirements
138	Load Personnel Data/Directory
139	Load Customer Data/Directory
140	Load Vendor Data/Directory
141	Develop Delegation/Designation of Authorit
142	Develop Escalation Procedures
143	Develop Emergency Notification Procedure
144	Document Recovery Locations
145	Document Other Alternate Sites
146	Prepare Work Area Recovery Procedures
147	Prepare LAN/WAN/PC Recovery Procedur
148	Prepare IS/IT Recovery Procedures
149	Document Off-site Storage Procedures
150	Prepare Data Recovery Procedures
151	Prepare Data Restoration Procedures
152	Walkthrough Indiv Team Recovery Procs
153	Review Prevention Phase Actions
154	Review Response Phase Actions
155	Review Resumption Phase Actions
156	Review Recovery Phase Actions
157	Review Restoration/Return Phase Actions
158	Gather Associated Documentation



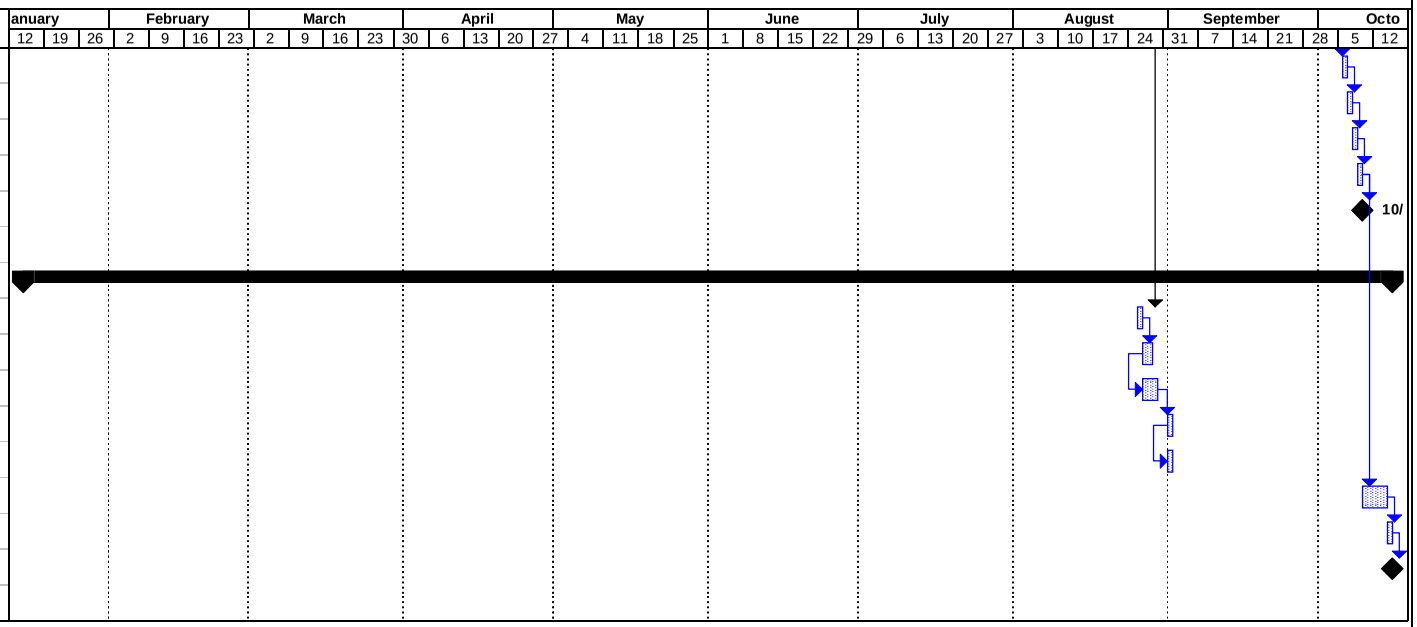
Example of a Business Continuity Plan Development Project

ID	Task Name
159	Validate Info Compiled into Databases
160	Print Plan
161	Review Business Continuity Plan (First Draft)
162	Phase 5 Complete
163	
164	**PHASE 6--TRAINING & CORPORTE AWARENES**
165	Establish Corporate Awareness Program
166	Establish BCP Training Program
167	Develop Definitions of Terms
168	**Provide Training to BCP Teams on:**
169	BCP Methodology
170	BCP Plan Development
171	Plan Assumptions
172	Plan Limitations and Scope
173	BCP Program Objectives
174	Key Disaster Scenarios
175	BCP Plan Exercise Procedures
176	BCP Plan Evaluation Procedures
177	BCP Plan Maintenance Procedures
178	Develop General Employee Awareness Prograı
179	Phase 6 Complete
180	
181	**PHASE 7--EXERCISES & TESTING**
182	Establish Exercise Program Objectives
183	Review Test Approaches
184	ID Test Planning Steps
185	Determine Logistics
186	Schedule Exercise Participants
187	Develop Exercise Scenario
188	Develop Exercise Scripts
189	Develop Segment Handouts
190	Conduct Structured Walk-through



Example of a Business Continuity Plan Development Project

ID	Task Name
191	Review Exercise Results
192	Critique Exercise
193	Write Exercise Report
194	Present Recommendations
195	Phase 7 Complete
196	
197	**PHASE 8--PLAN MAINTENANCE & UPDATES**
198	ID Sources of Change
199	Define Maintenance Procedures
200	Document Plan Maintenance Guidelines
201	Publish Plan Maintenance Guidelines
202	Implement Electronic Plan Maintenance Procs
203	Modify Plan based on Exercise Results
204	Publish Business Recovery Plan Changes
205	Phase 8 Complete
206	



Example of a Business Continuity Plan Development Project

ID	Task Name	anuary			February				March				April				May				June				July				August				September				Octo	
		12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	5	12
207	.																																						

APPENDIX 6

Example Scenarios

Scenarios should be specific and appropriate for each environment. They are used for testing, and requesting proposals from service providers.

1. A disaster incident affects your building such that no one is allowed to enter the building at the start of business tomorrow.
   - No one goes in or out of the building.
   - No data goes in or out of the building.
   - No telecommunications go in or out of the building.

   Duration of the outage—The building and facilities are unavailable for at least one month to six weeks.

2. Fire sweeps through the computer room causing total destruction. Disaster declared. Both the hot site and cold site are activated. The hot site is accommodated for 10 days before all systems are operative at the cold site. With the exception of your most valuable technical person, all personnel are available for recovery. Therefore, it is decided to utilize the technical expertise of both the hot site and drop shipment vendor to assist in recovery (another cost).

   At cold site for 60 days. Used 20 work areas (work area contracts are an additional cost per work area).

3. The most critical piece of hardware (running the most critical software) is fried. Knowing that it will take at least five days to get another machine in and ready, you decide to activate the hot site. All personnel are available for recovery. It takes eight days to replace and ready the new hardware.

   At hot site for 10 days. No work areas used.

4. Isolated fire in the computer room. Halon dumped. All servers and a mid-range (or mainframe) are irreparable. Hot site vendor is called. All other systems are cleaned and operable in 24 hours. All personnel are available for recovery.

   At hot site for 14 days. No work areas used.

5. Environmental hazard causes inaccessibility to the Data Center for four days. All equipment is intact, and all personnel are available for recovery.

   At hot site for five days. Used 55 work areas.

APPENDIX 7

Things to Remember in Developing a Disaster Recovery Plan

1. Keep your plan simple, it does not need to be perfect. Remember, any plan is better than no plan at all!
2. After testing (twice yearly) update your plan as necessary. Do not wait! A disaster recovery plan is never finished, it evolves.
3. Stay flexible—a flexible plan may better prepare your organization. Do not assume just one disaster possibility.
4. Document the plan and other materials—a list of your primary vendors (and secondary vendors if the disaster hits the primary vendor as well) is a must.

Example Checklist

1. Ask yourself, how important is data integrity and access? What price are you willing to place on that data? What would you do if your office was hit by a power failure, natural disaster, sabotage, etc.?
2. Identify your risks. Determine cost vs. risk—is your office in a high risk area? For example, California is susceptible to earthquakes.
3. Create a plan that evaluates/encompasses the essentials and set priorities—the best way to proceed at this point is to create a matrix or chart containing your data and equipment, plus its level of importance. Other important factors, such as loss of building floors and areas, personnel, back-up power, etc., need to be listed as factors affecting your plan (this is different for every case depending upon your business).

   The matrix will allow you to come up with contingency plans based on what happens during a disaster. What this does is allow you to get as close as possible to multiple scenarios. Remember that time may not be on your side in a disaster, so saving everything may not be an option. You do not want to decide what is important during a fire or natural disaster (see Prioritizing Chart). An inventory of your data storage and/or other components, vendor contact information (24 x 7), and registered licenses will all be necessary in this stage. A hot site, either for data or the recreation of your computing environment, also needs to be considered.

Reprinted portions of Giga Information Group Document No. 228970-MA98, Michael Adams, by permission

Prioritizing Chart

Priority	Definition
Critical applications	Must be recovered within 24 hours
Secondary applications	Must be recovered within 48 to 120 hours
Non-critical systems and applications	No effect upon ability to continue business operations

4. Inform your employees and develop a disaster team—this is often overlooked in a disaster recovery plan. Employees need to know what to do in the event something goes wrong. A disaster recovery team should have an identified leader and second-in-command. The remaining members of the team should be familiar with where the company's data resides as well as the software and hardware components involved.
5. Test your plan (twice yearly)—when you simulate a disaster, select a solution from your matrix (created in step 3). This is a critical stage because you need to prove that your plan works. If it fails, scrap it and devise a new plan of action. Practice makes perfect, and when your business is faced with a disaster you will be glad you tested your disaster recovery plan.
6. Go over results with the disaster team and employees and make the necessary changes—this will provide good analysis and expose the flaws in your plan. Changes will be become obvious while your recovery is taking place. Necessary changes will also include areas such as hardware/software upgrades and growth of the company in general. Major changes also should involve employee and disaster team notification.

Reprinted portions of Giga Information Group Document No. 228970-MA98, Michael Adams, by permission

APPENDIX 8

Example of a Plan's Contents

Remember, there is no "fill-in-the-blank" template for recovery plans. Each environment requires its own tailor-made design. This example, if used, should be customized for your agency.

Introduction — Why, elements, broad purpose.

Instructions — When is it activated, how is it distributed.

Document Organization — Major organizational plan units.

Distribution and Amendments — Who receives whole plan, who receives parts and which parts, future updates.

Mission Statement — Cultural values vital to plan mission success.

Policy and Objectives — Purpose defined.

Scope — Limits of plan.

Assumptions — Understandings.

Declaration Sequence — Steps taken after event ending in disaster declaration. Procedures, declaration form. Flowchart is good for this.

Alert/Notification/Activator Procedures — Process for all disruption notifications.

Maintenance and Testing — Responsibilities.

Outside Support — List of outside support required, i.e., security, etc.

Calling — Procedures for calling teams, including suggested scripts.

Usage — How will plan be used.

Coordinator — Responsibilities.

Definition of Terms — Glossary.

Skills — Grouping of available skills if needed during recovery.

Application Priorities — Most critical, order of recovery.

Assembly and Command Centers — Where will teams meet? Where is management team's command post?

Alternate Site — Hot site, cold site, etc. Backup sites and directions.

Communications — Voice and data end-points for organized restoration.

Recovery Teams — Who. Alternates. Duties.

Disaster Scenarios — Potential events.

Strategies — Planned actions for recovery process selection based on severity of outage.

Critical Vendors — Contacts for most important vendors during first 48 hours.

Forms — Sample forms to be used, dependent on disaster, press release, etc.

Pre-printed — List and samples. Include vendors, where stored off-site, how long to get printed and delivered.

Facility Layout — Scaled map of functional areas floor space to be used.

Call Lists — List of teams. Who will notify whom. Alternates. List of non-team staff members needing notification. Who calls.

Tasks — Tasks by teams during recovery.

Functions/Applications — Functions to the prioritized applications.

Computer Operating Procedures — Probably already exist. Can be referred to and location identified.

Site Requirements — Defines electrical, floor loading, etc. Blueprint-type details recommended. May be separate document.

Facilities — List of all. Current, off-site storage, alternate site, etc. Driving directions to each.

Personnel — List of all staff, with skill, location, office phone, beepers, home address, home phone, who to notify in-case-of-emergency and their phone.

Vendors — All doing business with, including phones, addresses, FAX, email, name, etc.

Computer Equipment — List of all currently installed equipment by name, number, specialized information.

Office Equipment — Furnishings and other equipment by name, numbers, specialized information.

Off-Site Data — List of all files stored off-site. Can be used as check list in case of disaster.

Software — List of packaged software, vendors information, outside support, etc.

Critical Documents — List most important documents for first 48 hours, copies, or instructions on where to find them.

Supplies — List of supplies required, especially first 48 hours.

Travel/Lodging — How handled. Through travel agency during crisis?

APPENDIX 9

Business Recovery Checklist

This appendix includes a business recovery checklist for each of the following:

- Process Owner
- Implementer
- Services

Business Recovery Checklist—Process Owner

1. Do you have a CRITICAL Business Process (CBP)?
2. Is a complete list of internal and external Service Providers (SPs) included in the disaster recovery plan?
3. Are there current service level agreements/documents of understanding with all SPs for this critical business process?
4. Are there documented disaster recovery plans for each critical SP for this critical business process?
   a. Are the plans stored off-site?
   b. Do the plans include all recovery information?
5. Has disaster recovery testing been conducted within the past 12 months?
   a. Testing within six months of a major change to the system or a critical application supporting a process?
   b. Were the critical non-computer sections of the process tested?
   c. Were both the computer and non-computer sections of the process tested by alternate site or backup personnel?
   d. Were SPs and other dependencies included in the test sequence?
6. Are critical application owners designing applications with "built-in" recovery and continuous operations/functions?
7. Are your SPs utilizing automated operations and/or remote operations, and are they trying to eliminate and/or minimize human dependencies within the processes/services/functions?
8. In case of a disaster, is there a prioritized notification procedure established to inform our owners and users of the situation? Has it ever been tested? Are SPs included in your notification process?

Business Recovery Checklist—Implementer

A. Management Issues

1. Have you fully analyzed your critical business processes' exposure to various types of threats and vulnerabilities?
2. Have you established recovery procedures to follow for each type of disaster?
3. Have you conducted a simulated disaster?
4. Are new or transferred employees immediately trained and apprised of their role in disaster recovery procedures?

B. Personnel Issues

1. Do your disaster recovery plans include the scheduling of personnel in case of a disaster?
2. Has a recovery directory been prepared that lists, in priority sequence, the critical personnel?
3. Is the recovery directory in easily accessible off-site locations (taking into consideration privacy and document security)?
4. Does the recovery directory include
   a. Each key employee's address and telephone number?
   b. Each key employee's position title and skill profile?
   c. Other personal information that may be useful in an emergency?
   d. SP address and emergency telephone numbers?
5. Have emergency transportation/lodging procedures been established? Are backup personnel available?
6. Have personnel been cross-trained on each other's duties and equipment?
7. Have backup personnel been identified, in case of casualty, for continuity of management and operations?
8. Are all backup personnel properly trained in their respective duties?
9. Have you addressed support for the families of personnel performing your recovery?
10. Do you have 24-hour access to key personnel and their alternates (local- and wide-area pagers, cellular phones, laptops, etc.)?
11. Have accommodations been made for people with special needs and provisions made for them?

C. Hardware

1. Have you kept a complete and accurate inventory of all supporting equipment including
   a. Special device(s)?
   b. Forms-handling equipment such as bursters, check signers, and decollators?
   c. Personal Computers (PCs), PC software and copiers?
   d. Special printer fonts and forms (invoices, checks, etc.)?
   e. Telephones
   f. Fax
   g. Dial-up capability port requirements
2. Is this inventory part of your business process recovery plan?
3. Is proximity to these items and your personnel an issue?

D. Disaster Recovery Information Protection

1. Have you evaluated the types of threats and vulnerabilities that your records/files may possibly be exposed to, such as
   a. Mechanical malfunctions?
   b. Updating of wrong file?
   c. Lost files?
   d. Theft of records?
   e. Criminal activity?
   f. Loss by natural disaster?
   g. Physical transportation accidents?
   h. Loss by moisture, mildew, mold, etc.?
2. When you copy files for off-site storage, do you first check the copies for
   a. Readability?
   b. Accuracy?
3. Are your on-site and off-site media storage cabinets
   a. Fire resistant?
   b. Smoke resistant?
   c. Water resistant?
   d. Movable so that they may be relocated quickly in the event of disaster?
   e. Secure?
4. Do you insure that long-term off-site storage materials are inventoried and usable?

E. Documentation

1. Are copies of your disaster recovery plan kept at home(s), as well as stored as disaster recovery information (i.e., vital records)? Who knows where they are?

2. Does your recovery documentation include all information necessary to recover the CBP, such as:
   a. Key contracts?
   b. Procedures/instructions?
   c. Critical dependencies?
   d. Names/locations of service providers?
   e. Special forms and equipment?
   f. Personal computer information
   g. Service level agreement information?
   h. Etc.?

   3. Are your instructions/documentation complete enough so that a person who is not familiar with the process could execute it? When was this process last tested? Results?

4. Who is responsible for the control and security of this CBP disaster recovery documentation?

Business Recovery Checklist—Services

A. Facilities and Services

1. Is your communications system thoroughly documented? Is a copy of the documentation protected?
2. Depending on the critical nature of your communications system, have you considered the appropriate backup for the following systems/terminals?
   a. Stand-alone terminals?
   b. Concentrators?
   c. Modems?
   d. Transmission control units?
   e. Datasets?
   f. Terminals?
   g. Telephone system?

   3. Is the site dependent upon a single major service supplier for utilities and telecommunications (power, telephones, fax, fuel, etc.)?

4. If you lose telephone communications service, do you have alternate backup systems and procedures?
   a. Short-term?
   b. Long-term?
5. Has site management appointed a focal point for the telecommunications disaster recovery process?
6. Has the identification and prioritization of critical circuits been approved by the site services manager?

7. Is there a documented telecommunications disaster recovery plan? Is it merged with the site disaster recovery plan?
8. Are all critical telecommunications circuits identified with users annually?
9. Have critical backup circuits been tested annually? Date of last test? Results?
10. Has it been verified that the telephone company has routed alternate links in paths different from the primary link paths?
11. Do you have backup mail and delivery systems for the movement of critical items such as
    a. Customer/user reports?
    b. Paychecks?
    c. Accounts payable?
    d. Accounts receivable?
    e. Packages?
    f. Priority mail?
    g. Priority interoffice correspondence?
    h. Bills?
    i. Invoices?
    j. Customer correspondence, information/documentation?

B. Supplies

1. If your forms/supplies are destroyed, do you have an adequate backup quantity stored in a readily-accessible safe place?
    a. Printed forms or special fonts?
    b. Plain stock (single and multi-part)?
    c. Printer ribbons?
    d. Diskettes?
    e. Labels?
2. Have you established "emergency order" arrangements with your vendors? Do you have alternate suppliers for critical supplies and service?
3. Do you have an adequate quantity of forms/supplies on hand should your supplier be hit by a disaster? Do you have arrangements with multiple vendors for vital forms and supplies?
4. Have you made a complete list of forms/supplies with
    a. Specific order numbers?
    b. Name, address, and phone number of the vendor(s)?
    c. Sample copies of forms (size, color, stock, grade, etc.)?
    d. Densities, tracks and model numbers listed for computer input/output media (i.e., disks, diskettes, tape)?
5. Do you have secure off-site storage for backup forms?
6. Have you made provision for control of vital forms?

C. Computing Services

1. Does this process depend on a computing service? If yes, answer Questions 2–6.
2. What applications?
3. Do you have service level agreements with
   a. Internal computing?
   b. Critical application owners?
4. Will you receive the computing service if the computer operates from an alternate site?
5. Will you receive the computing service if you go to an alternate site?
6. Have Items 4 and 5 been tested successfully?
7. Do you have manual procedures defined? Have they been tested?

APPENDIX 10

Examples—Responsibilities And Teams

There is no "cookie-cutter" approach to business continuity planning and disaster recovery teams that will fit all organizations. Plans should not be dependent on specific individuals but on positions and functions. These are examples only. Remember that the types of teams and related responsibilities must fit your agency's requirements.

Senior Management

The protection and continuation of agency personnel, assets, and agency critical functions is the responsibility of senior management. Senior management's support and partnership is essential and critical. It provides the resources and cooperation that is necessary to a successful plan.

Business Continuity Planning Coordinator

- Makes sure the plan and all its parts are complete, tested, and current.
- Makes sure team members, recovery and agency personnel are trained appropriately to their responsibilities.
- Coordinates the efforts of the various teams and team leaders to see that the pre-planning tasks are accomplished.
- Reviews the disaster recovery plan testing program and schedules.
- Obtains all contact lists.
- Produces and distributes the disaster recovery manuals.
- Keeps files on all appropriate vendors.
- Performs internal audit functions to test security measures and business continuity plans and reports the results to management.
- Handles and helps solve problems that cross departmental lines.
- Reconfirms the recovery procedure with each participant and makes modifications as necessary.
- Chairs the planning meetings to see that everyone is headed in the same direction.

Team Components

Teams consist of project managers, experts, and functional area staff.

Project Manager

- Coordinates planning activities.
- Coordinate with other teams and the BCP coordinator.
- Understands advantages, disadvantages, and costs of available alternatives.
- Identifies viable recovery strategies within business functional areas.
- Consolidates strategies.
- Identifies vital records and off-site storage requirements and selects alternative facilities.
- Develops business unit consensus for recovery of critical functions and strategies.
- Presents strategies to management and obtains their commitment.
- Establishes meeting schedules.
- Defines and publishes objectives.
- Assigns tasks.
- Documents the results of meetings.
- Prepares and conducts presentations to senior management, employees, auditors, and regulators.
- Identifies the appropriate experts within the agency.

Experts and Functional Area Staff

- Demonstrate expertise in agency systems and functions.
- Provide expert knowledge of operations and help determine applications and procedures that are most critical in the event of a disaster.

BCP Planning Team(s)

Remember that Line Supervisors have a working knowledge of their areas.

Public Relations/Media Handling

Public relations is a critical activity during an emergency event. The media can make or break even the best of efforts by an organization. Only a qualified and

experienced public relations coordinator should be allowed to respond to media questions. This is an agency policy decision.

Special Coordinators and Special Teams

You may want to have special coordinators and teams to address specific needs:

- Local, and federal relations and emergency response organizations (Police, Fire, etc.).
- Liaisons with headquarters and other divisions of the agency.
- Any appropriate special groups identified by the agency
- Any need to employ the skills and expertise of BCP experts/ consultant.

Systems Experts

Experts in the various mainframe, midrange, and small operating system environments, including data processing operations, storage media management, printing management, and operating systems security.

Communications Specialists

Experts in communications platforms are a resource required in the planning process. Restoration of voice services is fundamental to the start-up of business operations. The technical internal and external equipment required to plan for alternative voice resources must be identified early in the planning phase.

Network Experts

They plan for the acquisition of network hardware, data communication, and external resources, directly affecting the recovery time frame.

Acquisition and implementation of network resources often require long lead times.

Financial Experts

Financial experts are participants in the business impact analysis and may also provide assistance in developing the project budget.

Business Function Representatives

Representatives from the organization's operations units provide the expertise needed to describe how the units function, determine what operations to recover, develop recovery strategies and procedures, and identify appropriate team members.

Vital Records Management

Legal requirements related to the management of vital records may or may not be clearly documented in the organization. Experts in managing vital records can help provide a focused effort that is compliant with applicable laws or regulations. In addition, the vital records expert can help in defining recovery criteria that might be integrated into the vital records program.

Restoration Resources

External agencies or companies for the restoration of facility, building contents, office equipment, data processing equipment, and magnetic and paper records.

Human Resources

Human resources functions include payroll, employee relations, and regulatory requirements.

Security and Safety

Security and safety team considers plans for action during an actual disaster event.

Risk Management

Risk management team mobilizes immediately following a disaster.

Equipment and Supplies

This team provides advance purchase agreements with primary and secondary vendors.

Transportation

The transportation team plans for the transportation needs of the disaster recovery and business continuity teams.

Crisis Management Representative

If an agency has a crisis management team that handles such specialized problems as criminal activity, product contamination, and hazardous waste spills, one or more representatives of that team should take part in the business operations recovery project.

Legal Experts

A legal representative should participate as a project team member to ensure that issues related to potential liabilities are addressed in the plan. Additionally, lawyers may perform contract review for purchased recovery services.

Clerical and Support Staff

Clerical and support staff handle the clerical work associated with the project.

Recovery Teams

Responsibilities should be spelled out in detail in each plan.

Team Leaders

Team leaders are responsible for team procedures and disaster recovery checklists.

Management Team

- Assists the BCP Coordinator in obtaining cooperation of all areas involved in recovery effort.
- Assists the BCP Coordinator in obtaining cooperation of outside agencies.
- Assists the BCP Coordinator in obtaining required funding.
- Ensures that all requests for information from media, etc., are referred to a designated spokesperson.
- Maintains record of events.

Customer Team

- Notifies team members of disaster.
- Assesses damage in accordance with procedures.
- Participates in facilities planning.
- Tracks schedule impact to project and reports to management, as requested.
- Develops start-up user plans.
- Reports recovery progress to management.
- Ensures that all requests for information from media, etc., are referred to a designated spokesperson.

- Maintains record of events.

Security Team

- Ensures that the disaster recovery effort does not result in unauthorized access to classified or sensitive information or violate company security requirements.
- Notifies team members of disaster.
- Coordinates with customer(s) to obtain disaster-related security requirements and waivers.
- Monitors implementation and management of physical and logical access controls at alternate sites.
- Monitors declassification and removal of hardware and media.
- Ensure that all requests for information from media, etc., are referred to a designated spokesperson.
- Maintains record of events.

Facilities Team

- Notifies team members of disaster.
- Establishes disaster recovery operations center.
- Assesses damage in accordance with procedures.
- Participates in determination of salvage dispositions.
- Participates in monitoring of cleanup.
- Establishes staging area for salvageable items.
- Prepares list of equipment and services needed for restoration of disaster site.
- Coordinates with administrative support and purchasing teams as required in the acquisition of needed equipment and services.
- Develops estimate of time required to restore the disaster site to full capability.
- Maintains record of events.

Hardware Team

- Obtains and/or salvages computer and telecommunication hardware to meet minimum processing needs.
- Restores full processing capability.
- Notifies team members of disaster.
- Assesses damage in accordance with procedures.
- Participates in determination of salvage dispositions.

- Contacts vendors.
- Defines requirements for needed hardware.
- Coordinates with software team in workstation configurations.
- Ensures that all requests for information from media, etc., are referred to a designated spokesperson.
- Maintains record of events.

Telecommunications Team

- Reestablishes the voice/data telecommunications network
- Establishes telecommunications capability for backup restoration.
- Notifies team members of disaster.
- Assesses damage in accordance with procedures.
- Participates in determination of salvage dispositions.
- Orders equipment and services, as needed.
- Performs installation of replacement equipment.
- Supervises testing.
- Coordinates with voice data system vendor, as required.
- Coordinates and monitors the switching of circuits and lines to provide communications to the alternate processing site(s).
- Reviews, analyzes, and solves network problems.
- Ensures that all requests for information from media, etc., are referred to a designated spokesperson.
- Maintains record of events.

Applications Software Team

- Restores information processing services sufficient for continuation of vital business functions.
- Notifies team members of disaster.
- Assesses damage in accordance with procedures.
- Analyzes the status of processing at the time of the interruption.
- Coordinates with the BCP coordinator in determining priorities for running applications in disaster recovery mode.
- Contacts appropriate suppliers and vendors in order to determine when required equipment, software, and new license access keys will be available.
- Coordinates retrieval and use of backup data.

- Assists customers in implementation of manual backup procedures, when feasible.
- Works with programming staff.
- Coordinates with hardware team on server and workstation configurations.
- Coordinates with impacted customers in order to minimize their impact.
- Ensures that all requests for information from media, etc., are referred to a designated spokesperson.
- Maintains record of events.

Systems Software Team

- Establishes a working version of the operating and control systems, utilities, and general purpose software on the backup site computer(s).
- Notifies team members of disaster.
- Assesses data position.
- Assesses damage in accordance with procedures.
- Obtains operating system(s) program listing.
- Obtains backup media.
- Identifies backup configurations to be used.
- Verifies that all operating systems are loaded and tested.
- Verifies that telecommunications facilities are operational.
- Assists applications software team in restoring applications to the most current backup status.
- Accommodates hardware/software compatibility problems.
- Monitors processing.
- Ensures that all requests for information from media, etc., are referred to a designated spokesperson.
- Maintains record of events.

Administrative Support Team

- Provides supplies, food, shelter and transportation to the disaster recovery organization, as needed.
- Provides accounting and administrative support during the recovery effort.
- Notifies team members of disaster.
- Informs corporate purchasing, risk management, legal division subcontracts, and other relevant organizations of the need for actual/potential support requirements.

- Prepares and maintains a priority matrix of all support requirements against the various sources of support.
- Communicates and records all internal and external requests and orders for supplies and logistic support, including expected times and dates of delivery of supplies and performance of services.
- Provides purchasing team with a list of critical items which must be expedited.
- Provides disaster recovery team leaders with the accounting charge numbers and any other procedures necessary.
- Prepares and process purchasing documentation.
- Monitors disaster recovery effort costs.
- Ensures that all requests for information from media, etc., are referred to a designated spokesperson
- Maintains record of events.

Emergency Response (Crisis Management)Team

Senior managers are responsible for immediate response to crisis events. Therefore, they are normally part of the Emergency Response Team or Crisis Management Team.

The Emergency Response or Crisis Management Team

- Identifies the existence of emergency response procedures.
- Recommends the development of emergency procedures where none exist.
- Integrates disaster recovery procedures with emergency response procedures
- Identifies command and control requirements of managing an emergency.
- Recommends the development of command and control procedures that clearly define the roles, authority, and communications processes necessary to manage an emergency.

APPENDIX 11

Disaster Recovery Service Vendors: Tips, Check Lists, and Examples of Requests for Proposal

The tips, checklists, and proposals shown in Appendix 11.A, Appendix 11.B, and Appendix 11.C are EXAMPLES. They are NOT intended to be used as TEMPLATES. It is the responsibility of the agency or university to meet the state's purchasing and legal requirements and its own internal purchasing policies and procedures.

APPENDIX 11.A

Tips and Check Lists

Vendor Experience

1. How long has the vendor been in disaster recovery services?
2. Does the vendor have services other than disaster recovery, and if so, what is the ratio of the business?
3. What is the vendor's record in actually recovering organizations? How many? What type (full network, applications, etc.)? Time?
4. What are some of their past recovery problems?
5. What is customer satisfaction after disaster declaration?
6. Is there a customer satisfaction survey from the vendor and is it available?
7. Who are the other vendors they work with (paper, off-site storage, etc.)?
8. What are related services that are provided (mailings, etc.)?

Logistics

1. What type of recovery solutions are available at the hot-site facility?
2. What and where are the vendor locations?
3. What would be your assigned location?
4. How many customers do they current serve? How much growth do they anticipate?
5. What is facility access like (security, parking, convenience)? Are you guaranteed access?
6. What about multiple disasters? What are subscribers rights? Priorities? First come, first serve? Have non-subscribers ever been allowed to recover after a disaster? If so, what are the rights of subscriber as first? Provide a list of all subscribers who have preemptive rights?
7. Are there limits to number of customers per hot site? Can this be verified?
8. Where is second site, if primary is occupied to capacity?
9. Are any sites located in areas high risk areas?
10. Can the you notify the vendor of a potential disaster without a declaration fee?

Sites

1. In case of major regional disaster, it is likely that all vendors would experience resource shortages.
2. UPS? Dual power supply (generator and UPS)?
3. Backup telecommunications? (VSAT, microwave, etc.)
4. How and what is used for fire protection?
5. Cold site space also available?
6. The facility can handle how what types of additional personnel (operations, programming, users, applications, etc.)? Does the site have personnel to perform these types of functions? If so, what is their qualifications and how are they available?
7. What is to be expected from multiple area disaster? Will you have to reduce support and service level? Share CPU?
8. Square feet for use? For cold site if also provided at site?

Testing

1. What are the average number of tests per site per month?
2. When will your first test be conducted? Prime shift?
3. Allow for special tests in addition to the minimum number of tests you need.
4. What is cost of exceeding allotted test time?
5. For mainframe users, six, eight-hour blocks are standard, but this is quite negotiable. Have the provider bring out the testing calendar and get commitments before signing a contract.
6. Is testing on equipment not in your contract allowed?
7. If testing is bumped because of a real disaster, how do they reschedule? What is their policy?

Technical

1. Are your circuits connected full-time to front-end processors? Are they immediately switchable?
2. Can testing be conducted remotely from any location you designate?
3. Does vendor provide network consulting for backup? If so, what are the fees?
4. What local loop routing is provided and by whom?
5. What types of access (T1, live dial tones, etc.)?
6. Who are the carriers providing service to the hot sites?
7. Are CPUs for customers physically or logically partitioned? Know details on each.
8. Is an electronic vaulting program available?

9. If your equipment or building is damaged, can the vendor provide assistance with salvage or restoration? Access to mobile sites? Obtaining new equipment?

Contracts and Costs

1. Does the vendor accept liability for damages caused by them? If so, are there monetary limits? If so, what is the limit?
2. Technical support during recovery guaranteed?
3. Can you audit the recovery center and is this included in contract?
4. Independent audit done regularly on vendor contracts and compliance? If so, is a copy provided to you? If not, what is justification not to do so?
5. Strive to make vendor evaluations consistent.
6. Vendor prices are almost always negotiable. Longer term contracts usually mean lower prices. Cancellation Clauses—contracts typically have severe penalties that tie users to a five-year term. These contract terms are negotiable, and elimination of these penalties can be crucial to client enforcement of vendor performance. Make sure you cover your organization's future growth needs in long term contracts.
7. Declaration/Usage Fees. Rates are negotiable but may be immaterial unless clients plan to declare preemptively under threatening conditions (this is what a declaration fee is designed to prevent). Make sure you understand declaration policy and fee. Know both hot and cold site usage fees.
8. Make sure any agreed to changed in contract are in writing.
9. Get not-to-exceed prices that will cover your growth for the life of the contract. Vendors have charged up to triple the initial price per MIPS for incremental capacity. Also, agree on processor capacity ratings before signing.
10. Understand your disaster recovery service provider's equipment profile with respect to your own specific needs. Get written commitments from your provider to grow their processing capabilities as your capacity requirements grow over the life of the contract. Get not-to-exceed prices for specific capacity tiers. Forward unit pricing should track downwards at prevailing industry rates.
11. Agree on a basis for processor capacity ratings and include it in the contract for both current and yet-to-be-announced processor offerings.
12. Solicit disclosure on what other customers the disaster recovery service provider has in your risk area (same building, same flood zone, etc.) as at least one vendor has been caught overselling their capacities in the past. Get written guarantees on how the vendor will reconcile resource conflicts.
13. If services are included in proposals, have vendors' professional-services personnel interview with your technical-support staff to validate their credentials. If vendors seek a price premium on disaster recovery planning assistance, break out these services and bid them separately against independent consulting firms specializing in disaster recovery planning.

14. Understand what testing times will be made available to you before signing any contracts. Try to establish a testing schedule for the life of the contract.
15. Do not agree to significant cancellation penalties. These terms are negotiable (but usually hard fought) and critical to ensuring competitive pricing and quality service for the life of the contract.

In case of major regional disaster, it is likely that all vendors would experience resource shortages.

Additional Reference for Requests for Proposals:

http://www.networkcomputing.com/1001/1001f1.html (subject to change)

"Heading for Disaster?" Series of articles on the Network Computing web site. It highlights disaster recovery RFPs. The articles include vendors side-by-side responses and the complete architecture, connectivity, and cost comparison chart.

Sources: Giga Information Group, Disaster Recovery Institute, Auerbach Publications

APPENDIX 11.B

Example One: Request for Proposal

[Cover Letter]

<DATE>

<INSIDE ADDRESS>

Dear Vendor:

Agency/University, whose headquarters is located at <ADDRESS>, is currently engaged in Disaster Recovery Planning for its data center located at <ADDRESS>. Part of this planning is to evaluate selected hot site vendor's ability to provide recovery capabilities in the event of a disaster. We wish to consider *Agency/University* and invite you to submit a response to this Request For Proposal.

The attached document represents You Organization's technical requirements for disaster recovery hot site and cold site services.

We look forward to receiving a proposal from *Agency/University*.

Sincerely,

<NAME>
<TITLE>

TABLE OF CONTENTS

Agency/University

REQUEST FOR PROPOSAL

DISASTER RECOVERY SERVICES

I. INTRODUCTION

A. Purpose

Agency/University has completed an analysis of existing business application and determined those which are critical in nature and would need to be supported at an alternate facility in the event of a disaster. *Agency/University* has made a determination of the facility requirement and system configuration, which we feel, is adequate to provide necessary backup for these critical applications.

In the event of a disaster, *Agency/University* intends to resume processing of these critical application within <TIMEFRAME> hours (Recovery Time Objective).

As a result, *Agency/University* has issued this Request For Proposal for disaster recovery services. The intent of this document is to define the parameters and requirements of the desired disaster recovery services based on the following objectives:

1. <INSERT DATA>
2. <INSERT DATA>
3. <INSERT DATA>
4. <INSERT DATA>

B. Corporate Overview

<INSERT DATA>

C. Recovery Configuration Specifications

Detailed below is the minimum system configuration to support the recover *Agency/University*'s business systems environment.

1. Computer Hardware

QTY	*DESCRIPTION*
(___)	<MAKE/MODEL> Central Processing Unit
	___ MIPS
	___ Megs Main Memory
	___ Megs Expanded Memory
	___ Channels
(___)	<MAKE/MODEL> Front End Processor
(___)	<MAKE/MODEL> Disk Controllers
(___)	<MAKE/MODEL> Disk Drives (___ Addresses)
(___)	<MAKE/MODEL> Disk Controllers
(___)	<MAKE/MODEL> Disk Drives (___ Addresses)
(___)	<MAKE/MODEL> Disk Controllers
(___)	<MAKE/MODEL> Disk Drives (___ Addresses)
(___)	<MAKE/MODEL> Tape Drive Controller
(___)	<MAKE/MODEL> Magnetic Tape Cartridge Units
(___)	<MAKE/MODEL> Tape Drive Controller
(___)	<MAKE/MODEL> Magnetic Tape Reel Drives
(___)	<MAKE/MODEL> Line Printers
(___)	<MAKE/MODEL> Laser Printers
(___)	<MAKE/MODEL> Communications Controllers
(___)	<MAKE/MODEL> Communications Controllers
(___)	<MAKE/MODEL> CRT Terminals
(___)	<MAKE/MODEL> CRT Terminals
(___)	<MAKE/MODEL> CRT Terminals
(___)	<MAKE/MODEL> CRT Terminals

2. Communications

<INSERT DATA>

A network diagram has been included as Exhibit <NUMBER>

3. Operating Systems Software

<INSERT DATA>

4. Test Time

Bidder shall provide test time for each contract year. Test time shall be included in the proposed hot site services. Vendor will provide at least <NUMBER>% of the specified recovery configuration for testing.

5. Cold Site

Vendor shall be capable of providing a cold site for the purpose of:

a. Supporting *Agency/University*'s required system configuration for an extended period of time. It is preferable that the cold site be collocated with the hot site facility.
b. To support the immediate addition of the following equipment:
<INSERT DATA>
<INSERT DATA>
<INSERT DATA>
c. <INSERT DATA>

Agency/University shall be granted access to the cold site facility within <NUMBER> hours after notification and occupancy shall be at least twelve (12) months.

II. PROPOSAL PREPARATION/SUBMISSION

All vendors shall adhere to the following schedule and sequence of events in preparing and submitting a proposal in response to this Request For Proposal:

A. Scope of Work

Each vendor will propose to provide disaster recovery services to *Agency/University*.

B. Request For Proposal

This document is a Request For Proposal (RFP) and does not necessarily represent *Agency/University*'s final requirements. *Agency/University* reserves the right to supplement or amend the RFP, giving equal information and cooperation to all bidders with respect to such amendment. Further, *Agency/University* reserves the right to waive any requirements specified herein if, in its opinion, such waiver would be in the best interest of *Agency/University*.

The cost associated with developing this proposal shall be borne solely by the vendor and shall not be reimbursable by *Agency/University*.

The term "bidder" and "vendor" is used interchangeably and in all cases refers to the vendor responding to this RFP.

C. Issued

This RFP is being issued to selected vendors as of <DATE>.

D. Bidder's Conference

A mandatory bidder's conference is being held on <DATE>. Each attendee must be pre-registered no later than <DATE>. *Agency/University* will issue responses to all questions raised at the bidder's conference within seven (7) days following the conference.

The conference is being held at <TIME> at the following location: <INSERT ADDRESS>

Attendees must contact <NAME> at <PHONE> for pre-registration.

E. Questions

During the proposal preparation period, questions should be directed to the following individual(s).

Hardware:	<NAME> <TITLE> <PHONE> <FAX>
Telecommunications:	<NAME> <TITLE> <PHONE> <FAX>
All Other:	<NAME> <TITLE> <PHONE> <FAX>

F. Delivery of Proposals

Bidders shall submit <NUMBER> complete copies of their proposal no later than <TIME> on <DATE>. *Agency/University* reserves the right to refuse any proposals received after this time.

Proposals must be submitted to:

<NAME>, <TITLE>
<COMPANY NAME>
<STREET ADDRESS>
<CITY/STATE/ZIP>

All materials submitted in the bidder's proposal become the property of *Agency/University* and will not be returned.

Each proposal must follow the mandatory proposal format as outlined in Section III, Vendor Instructions.

G. Modification of Proposals

Modifications to a submitted proposal will be accepted in writing prior to the scheduled submission cut off date and time as specified in Section II, Paragraph F of this RFP.

H. Withdrawal of Proposal

Bidders may withdraw their proposal at any time by submitting written notice of withdrawal prior to the scheduled submission cut-off date and time as specified in Section II, Paragraph F.

I. Acceptance or Rejection of Proposals

Agency/University reserves the right, at its sole discretion, to accept or reject any or all proposals, wholly or in part; to waive any technicality in any proposal; and to make awards in a manner deemed in the best interest of *Agency/University*.

J. Selection of Vendor

All bidders will be notified of *Agency/University*'s decision on or before <DATE> unless unforeseen delays, such as the need for additional analysis occur.

K. Contract Award

The contract, if a proposal is accepted, will become effective following review by *Agency/University*'s legal counsel and approval of *Agency/University*'s senior management and other appropriate personnel.

L. Timeframe

Request For Proposal Issued:	<DATE>
Pre-Registration Bidder's Conference Deadline:	<DATE>
Deadline for Questions:	<DATE>
Bidder's Conference:	<DATE>
Distribute Bidder's Conference Minutes:	<DATE>
Proposals Due:	<DATE>
Bid Awarded:	<DATE>
Contract Start Date:	<DATE>

M. Proprietary and Confidential

The information contained within this RFP is both proprietary and confidential to *Agency/University*. Bidder shall not duplicate or distribute this RFP to any individual or company, unless said individual or company is directly involved in the completion of bidder's response.

III. VENDOR INSTRUCTIONS

A. General Instructions on Proposal Format

To simplify the evaluation and selection process, the submitted proposal must be prepared following the order of Section IV Technical Specifications and Requirements. *Agency/University*'s evaluation process incorporates the placing of a weighted point value upon each item of information specifically requested in this bid document. Failure to complete and follow the response format in the required sequence, even if addressed elsewhere in the proposal document, may result in the proposal being rejected by *Agency/University*.

Bidder's response must include the RFP question followed by bidder's response.

B. Special Instructions

1. Services

Vendor shall provide hot site services. Vendor shall provide access to the hot site facility within <HOURS> after notification. Following a declared disaster, *Agency/University* shall be permitted to occupy the hot site for a period of up to six (6) weeks.

2. Contract Term

Vendor shall provide pricing for <NUMBER> year term(s).

3. Price Guarantee

By submitting a response, vendor guarantees that all cost information provided shall be valid for a period of ninety (90) days.

IV. TECHNICAL SPECIFICATIONS AND REQUIREMENTS

Specific information concerning the services and facilities being proposed by the vendor is contained in this section of the Request For Proposal.

Bidder's proposal *must* respond to each point, whether vendor can or cannot meet the requirement. If any requirement cannot be met, a full explanation must be given, and, if appropriate, an alternative solution proposed.

A. Vendor Profile

1. Vendor Corporate Profile

This section must provide a brief overview of vendor's company, including discussion of:

- History
- Organization and Corporate Synergy
- Mission Statement

2. Experience

a. How many customer declarations has vendor supported to date?
b. How many non-customer declarations has vendor supported to date?
c. How many customer tests has vendor supported to date?

3. Customer Base

At present, how may subscribers does vendor currently support?

4. Sharing of Recovery Facility

a. What is vendor's policy on handling the recovery of multiple subscribers when both contracted for the same recovery hardware i.e. CPU sharing?
b. Does vendor allow sharing by more than one subscriber of the same recovery facility?

5. Multiple/Regional Disaster Support

a. What is vendor's policy on regional disasters or multiple, simultaneous disasters when more than one subscriber invokes a disaster declaration?
b. Can vendor provide access to additional hardware at time of disaster? What rights to access are granted to *Agency/University*

6. Disaster Avoidance

What is vendor's methodology and capability to provide disaster avoidance support?

7. Testing Methodology and Support

a. Provide a summary of vendor's testing methodology and standard support provided during tests.
b. What type of support does vendor provide before, during and after a test? What type of fee is associated with this support?
c. Does vendor support remote testing?
d. Does vendor provide turnkey services?
e. What additional fees will subscriber incur during testing or disaster recovery (i.e. telephone expense, etc.)?

8. References

Each bidder must provide three (3) references of customers currently under subscription for a disaster recovery configuration.

9. Financial Data

This section should contain information describing the current financial condition of vendor's company. Include bidder's latest annual report.

B. Staff and Services

1. Support Staff Availability

Indicate the number of support staff personnel (and their position) on site during testing and disaster recovery.

2. End-User Support Area

Describe the end-user support area available with a hot site and cold site subscription for *Agency/University* personnel. Is this area shared with other customers?

3. Support Services

Describe what type of support services vendor provides as part of their contract and what types of support services are available for an additional fee.

C. Recovery Configuration

Vendor shall detail their proposed hardware, telecommunications coldsite and testing recovery configuration below. Vendor shall provide a line by line comparison between the required recovery configuration detailed under Section I Introduction, Paragraph C, Recovery Configuration Specifications and their proposed configuration.

If a specific requirement cannot be met, vendor shall explain why and if applicable, offer an alternative solution. Vendor shall also provide details regarding optional services available.

This section of the proposal shall not contain any cost data. All cost data shall be included under Paragraph D. Proposed Pricing.

Agency/University's Required Recovery Configuration		*Agency/University*'s Proposed Recovery Configuration	
Qty	**Description**	**Qty**	**Description**

D. Proposed Pricing

Vendor shall provide pricing for <NUMBER> year term(s) for the proposed recovery configuration in format indicated below. Vendor shall also include pricing for all optional services proposed. Pricing shall include the monthly subscription fee, disaster declaration fee, daily usage fees and any other associated fee (including one-time fees).

Proposed Pricing			
Service	**Term**		
	X Year	**X Year**	**X Year**
Hot Site Services Monthly Subscription Disaster Declaration Daily Usage Annual Test Time			
Cold Site Services Monthly Subscription Disaster Declaration Daily Usage			
One-Time Fees (detail)			
Optional Services (detail)			

E. Terms and Conditions

1. Contract

Vendor shall include a copy of the contract for *Agency/University*'s review.

2. Upgrades

Provide vendor's provisions for upgrading *Agency/University*'s recovery configuration during the term of the contract.

3. Automatic Renewal

a. What is the length of term of the automatic renewal?
b. Does the vendor provide notice prior to the automatic renewal?

F. Vendor Policies

1. Geographic Priority Access

Provide vendor's policy for preventing *Agency/University*'s right of access to the primary recovery configuration to be pre-empted by another subscriber.

2. Pre-Emptive Access Rights

Is vendor currently engaged in a contract that allows a customer(s) to have greater access rights than *Agency/University*

3. Disaster Alert and Declaration

a. Define vendor's disaster alert and declaration procedure.
b. Does vendor require a fee be paid when placing a disaster declaration or alert?
c. Does vendor require subscribers to place a disaster declaration in order to "reserve" a recovery facility?
d. How does vendor assign a recovery facility when a subscriber places a disaster declaration?

4. Subscriber Risk Limitations

a. How does vendor agree to limit the risk of simultaneous declarations from multiple subscribers of the same configuration size of *Agency/University*
b. How does vendor assure that frivolous disaster declarations are not made?

G. Recovery Facility Specifications

1. Location(s) Available

a. Provide a list of all vendor hot site recovery facility location(s).
b. Provide a list of all cold site facilities.
c. Provide a list of all work area recovery facilities.

2. Telecommunications

a. Does vendor have their own internal backbone network?
b. What type of redundancy does your proposed facility have to the local exchange carrier?
c. Does vendor have direct access to any of the interexchange carriers?
d. Can *Agency/University* install a dedicated line into your facility, which is closest to our current data center and backhaul our bandwidth through your backbone network? If yes, how much bandwidth can we subscribe to for the purpose of backhauling?
e. Can *Agency/University* acquire dedicated bandwidth from vendor for our backbone network and then at time of disaster reroute the bandwidth to your recovery facility so that we can avoid having to acquire switched T-1 circuits?
f. How can vendor combine different recovery platforms located in different recovery centers to provide *Agency/University* with a total recovery solution?
g. Does vendor provide bridges, routers, multiplexors and channel extension capabilities at the proposed facility?

h. Can vendor's CNT equipment that is used to support your backbone network be subscribed to by *Agency/University*

i. What usage charges, if any, can be saved by using vendor's network capabilities?

j. Explain why vendor's networking capabilities provide a superior recovery solution to *Agency/University*.

k. Is vendor positioned for emerging technologies and high bandwidth needs such as ATM?

3. Facility Control

If any recovery facility is utilized for anything else besides disaster recovery, indicate the location of the recovery facility and explain its use.

4. Access/Occupancy

a. *Agency/University* requires access within <HOURS> after placing a disaster declaration. Can vendor meet this requirement?
b. *Agency/University* requires a minimum of six (6) weeks of occupancy in the hot site following a disaster declaration.

5. Fire Detection/Suppression System

Detail the fire detection and suppression system of the proposed recovery facility.

6. Security System

Detail the security system and security staff provided at the proposed recovery facility.

7. Environmental Equipment

a. Detail the environmental support equipment of the proposed recovery facility:
   1. Power conditioning
   2. HVAC
   3. Chiller
   4. UPS
   5. Diesel Generator

b. Indicate whether the proposed recovery facility has redundant capabilities for the above environmental support equipment.

8. Utility Vendors

a. Detail which utility (electrical and communications) vendors service the proposed recovery facility.
b. Indicate redundant capabilities for electrical and communications utilities in the event of an outage.

9. Customer Equipment

a. Describe provision for subscriber's placement of critical equipment, such as multiplexors, etc., at the recovery facility.
b. Will *Agency/University* incur a fee for placing customer owned equipment at the proposed recovery site?

10. Maintenance Procedures

What are the maintenance procedures for the recovery facility, hardware and environmental support equipment at the proposed recovery facility?

11. Geographical Location

What is the geographical location (i.e. urban or suburban) of the proposed recovery facility?

12. Transportation

Provide detail regarding local ground transportation and airport locations near the proposed recovery facility.

13. Lodging/Restaurants

How many hotels and restaurants are available within a five mile radius of the proposed recovery facility? Do the local area hotels offer corporate discounts to vendor's customers?

H. Additional Information

Vendor should include any additional information, which they feel would aid *Agency/University* in their review process. This information should be limited to information the vendor feels pertinent to their response, which was not specifically asked for in the Request For Proposal (i.e. marketing literature, additional support provided, optional services, etc). Vendor should be selective in the material to be included in this section.

V. APPENDIX

Note: This section is reserved for any additional documentation which customer wishes to include in this Request For Proposal (i.e. hardware diagrams, network diagrams, etc.) Any documentation included in this section should be reflected on the Table of Contents.

APPENDIX 11.C

Example Two: Request for Proposal

Request For Proposal

For

Hot Site Services

Agency/University

<DATE>

REQUEST FOR PROPOSAL
FOR
HOT SITE SERVICES

Agency/University would like <Vendor> to respond to the following Request for Proposal (RFP) for information about <Vendor> disaster recovery hot site services. The response should be carefully structured in the same format as the RFP. Respond directly to each item; if additional product offerings are available, please provide them via a separate attachment at the end of the proposal.

Timetable For Evaluation And Implementation

The following timetable for the RFP evaluation and implementation is anticipated. ***Agency/University*** reserves the right to alter the following timetable based on business conditions and circumstances:

Request for Proposal Release Date	<DATE>
Request for Proposal Response Deadline	<DATE>
Supplier Presentation (Optional)	<DATE>
Agency/University Evaluation Period/Selection	<DATE>
Contract Start	<DATE>

- We require three printed copies of the bid response.
- Send bid responses to ***Agency/University, 111 First Street, City, State 11111***.
- Fax all questions to name at ***xxx-xxx-xxxx***.
- Bids must be received by <TIME> on <DATE>. Bids may be sent via courier, certified or overnight mail. Please do not deliver RFP responses in person.
- In the event that modifications, clarifications, or additions, to the RFP become necessary, (Vendor) will be notified in writing.
- Bidders may be disqualified and proposals rejected for any of the following causes:
  - Lack of signature by an authorized representative on the RFP form.
  - Failure to properly complete the RFP.
  - Failure to meet the time criteria established.

Non-Disclosure

All information provided by ***Agency/University*** in connection with this RFP shall be considered confidential and proprietary information of ***Agency/University*** and must not be disclosed to individuals outside the (Vendor) organization without prior written approval. Any material submitted by (Vendor) that is to be considered confidential must be clearly marked as such and must include all applicable restrictions. All documentation and manuals submitted by (Vendor) shall become the property of ***Agency/University*** unless requested otherwise by (Vendor) at the time of submission.

Vendor Incurred Costs

All costs incurred in the preparation and presentation of this RFP in any way whatsoever shall be wholly absorbed by (Vendor).

Save Harmless

By submitting a proposal (Vendor) agrees to protect and save harmless ***Agency/University*** against any damage costs or liability for any injuries to persons or property arising from acts or omissions of (Vendor), its employees or agents, any of which result from the purchase or lease of goods or services form (Vendor) proposal.

Price Guarantee

Vendor must guarantee the prices quoted in the proposal will not increase for at least 90 days from date of proposed submission.

Not A Contract

THIS RFP IS NOT A CONTRACT AND DOES NOT IN ANY WAY BIND ***Agency/University*** TO ANY OBLIGATIONS OR IMPOSE LIABILITY FOR ANY COSTS OR EXPENSES INCURRED BY (VENDOR) IN CREATING THE PROPOSAL.

REQUIREMENTS FOR HOT SITE PROPOSAL

General

- The requirements that are provided in the document are the anticipated resource requirements as of <DATE>.
- The response to this proposal should include the resources, product offerings, and pricing that are in place as of today. Provide information bout new equipment or product offerings that may be in place by <DATE>, but do not base the proposal and pricing on future offerings.

CPU

- The CPU must be a minimum of a xxx-xxxx with xxx MB of real storage, xxx MB of expanded storage, and xx channels.
- The CPU MIP growth rate is projected to be xx% each year.

DASD

- xxx GBytes of DASD consisting of:
  3390 - # of addresses
- DASD must be behind (x) cashed controllers of the xxxx-xxx vintage.
- Growth in GBytes is projected to be xx% each year.

Tape

- xx# tape drives capable of reading IDRC compressed tape

Output Services

- (x#) IBM xxxx impact printer will be required.

Office And Workstation Area

- xx# workstations to accommodate technical staff personnel equipped with 3270 color terminals.
- xx# office spaces to accommodate project leaders and administrative personnel.
- Access to FAX machines, copying machines, and normal office supplies.

Staff Required

- Tape operators during testing and in the event of a declaration.
- Some technical assistance may also be needed during testing and at declaration.

Network Requirements

1. The network resources specified here reflect current level network configuration.

Quantity	Protocol	Line/Type	Speed	Modem	Dial Offices	Backup

********[FILL THIS INFORMATION IN]********

2. Network Hardware:

   Vendor will supply i.e. routers, FEP (Channels, LIC1, LIC3, High Speed Scanners, etc.) and any other unique network hardware (provide detailed configurations).

3. Network Diagram is being provided.

Test Time Requirements

- ***Agency/University*** will require xx hours of test time annually.

PROPOSAL BID RESPONSE ITEMS

Please respond to each item in the order that they are presented below.

1. Bidder Corporate Profile

Provide a brief overview of the bidding company and services, including description of:

a. competitive strengths,
b. description of company's primary business function and service,
c. corporate (parent) and other subsidiary or license affiliations (if applicable),
d. commitment to disaster recovery business,
e. the initial date recovery service was offered commercially,
f. market share,
g. size of customer base,
h. maximum number of subscribers allowed at each facility,
i. disaster recovery plan testing experience,
J. test time allowances and options for additional test time,
k. experience in actual disaster recovery incidents,
l. planned enhancements (additional recovery sites, new technology, configuration upgrades, etc.)
m. Financial Data—Provide information describing the current financial condition of vendor's company. Include bidders financial report.

2. References

A minimum of three bidders' clients must be provided as references, including the company name, address, and contact person, and contact's telephone number. The references should include at least one client who has used the bidder's services to recover from an actual disaster. The remaining references should have conducted multiple disaster recovery tests. These clients must be willing to discuss their experience with representatives of ***Agency/University*** .

3. Prime Contractor Responsibility

If the proposed services include the use of products or services of another company, ***Agency/University*** will hold the bidder responsible (as the prime contractor) for the proposed service(s). Specifically identify other companies that will be utilized. Indicate your compliance to this requirement.

4. Vendor Policies

a. How does vendor minimize the risk or handle simultaneous events from multiple subscribers that require the same equipment? Does vendor provide liquidated damages for failure to perform?
b. Vendor Integrity – Will the vendor allow a non-subscriber to declare and subsequently recover at the vendor's recovery facility? If yes, provide conditions when this might happen.
c. Sharing of the Facility – Does vendor share the recovery facility? If yes, how will vendor protect the confidentiality of "Your Organization's" data? If yes, describe physical and logical security measures taken when multiple subscribers are concurrently using the same customer suite. What are the obligations and options available if ***Agency/University*** does not agree to sharing arrangement?
d. Preemptive Access Rights – Will vendor allow any subscriber to have preemptive rights or preferred rights over ***Agency/University*** ? If yes, describe the circumstances.

5. Testing Methodology and Support

a. Provide detailed information regarding your testing methodology and standard support services provided during test exercises. This includes pre-test reviews, configuration change control and information synchronization between ***Agency/University*** and vendor configurations.
b. What support does vendor provide before, during and after a test? What type of fee, if any, is associated with this support? What is vendor's approach to partitioning? Physical, logical or software? How does vendor approach IOCP differences between customer and vendor configurations? What support does vendor provide to assist in this effort?

6. Hot Site/Cold Site Description

Please give details regarding the primary site selected and the alternate site available if primary site is occupied.

a. Describe general characteristics of the hot and cold site facilities including location, square footage, and the type of equipment currently in the hot sites at this time as well as equipment to be in the site by <DATE>.

b. Describe the local telephone company and inter-exchange carrier access installed at your proposed hot sites, which are suitable for recovering "Your Organization's" network. Provide information regarding access methods, standard telephone companies, and alternate access vendors. Describe any pertinent network recovery experience and capabilities.
c. Please describe vendor's capabilities for testing from location remote to primary recovery center.
d. Describe provision for subscriber's placement of their own critical equipment, such as servers, multiplexors, etc., at the recovery facility.
e. Describe proximity to hotels, restaurants, and airports.

7. Hot Site Environmentals and Physical Security

Describe in detail the physical security in place at hot site facilities (primary/alternate). Discuss hot site environmental capabilities including but not limited to the following systems:

a. Power feeder lines
b. UPS
c. Diesel backup
d. Smoke detection
e. Water detection
f. Fire suppression
g. Chilled water

8. Hot Site Staff

Indicate the number of support staff personnel on site (and their position) dedicated to ***Agency/University*** during test and disaster recover. How many additional personnel would be onsite and available to help ***Agency/University*** during testing and disaster recovery that are not exclusively dedicated to ***Agency/University*** .

9. Facility Audit

a. Will the vendor allow a representative of ***Agency/University*** or independent third party to audit the proposed recovery facilities?
b. Have your recovery centers been ISO 9001 certified? If so, domestic or international?
c. If not, are the vendor's facilities or processes audited annually? If yes, by whom?

10. Customer Support Process

a. If ***Agency/University*** decided to contract with (Vendor) for hot site services, describe how (Vendor) would initiate the process with ***Agency/University*** . What services would be provided, what recommendations would (Vendor) have for a new customer, and what activities would be important in the first year of business relationship?
b. What does (Vendor) feel is important to maintain a strong working relationship with clients after the first year of hot site services?
c. Define and describe the alert declaration process.
d. Define the normal process for upgrading to new hardware and moving to new software releases at the hot sites. Describe both the business philosophy and the actual mechanics involved.

11. Customer Solution and Pricing

a. How would (Vendor) meet the requirements of ***Agency/University*** as defined in this document? Be specific and base the pricing on the services defined in this section.

b. As ***Agency/University*** moves forward to implement new technology, both hardware and software, how would vendor assure ***Agency/University*** that the hot site will keep pace with our data center? Is (Vendor) willing to commit contractually to providing the hardware and software when needed by ***Agency/University*** ?

c. Provide a summary of (Vendor) subscription charges broken down into logical subcategories. Provide pricing information for a one, three, and five year contract. Submit a summary chart that is structured similar to the chart shown below:

	One-year Contract	Three-year Contract	Five-year Contract
3090, DASD, Tape	$xxx	$xxx	$xxx
OEM	$xxx	$xxx	$xxx
Network	$xxx	$xxx	$xxx
TOTAL	$xxx	$xxx	$xxx

NOTE: Please document discount amounts or percentages that would be applicable to ***Agency/University*** for each of the three contract options.

d. Define the charges for using the hot and cold sites during a declared disaster for each of the three contract options. Indicate the maximum stay in the hot site facility and provide the data in a format similar to that listed below:

One-year Contract:

- Declaration fee
- First 24 hours
- 24 – 48 hours
- Additional per day charge in the hot site
- Charge per day in a cold site

Three-year Contract: (Same format as the One-year Contract)

Five-year Contract: (Same format as the One-year Contract)

12. Contracts

a. Clearly define what services are not part of the basic contract and provide pricing for those services.

b. Please include as an addendum to this RFP, a copy of the standard (Vendor) hot site contract. Provide information about contract modifications that have been made for other customers and what contractual provisions (Vendor) would be willing to provide ***Agency/University*** if (Vendor) is selected to provide hot site services.

APPENDIX 12

Example Team Checklists

From these checklists, you can develop checklists for business units, support teams (e.g., HR, Legal, Procurement, Finance and Acctg., etc.) Note that there is great similarity in some areas.

Recovery Check List (Incident Management Team)

Note: Generally, this checklist is in sequential order, but actions can be done in parallel.

Action — Reference

EVENT OCCURRENCE

☐ **Incident Detection** — Page/Section

☐ **Incident Reporting** — Page/Section

☐ **Emergency Response** — Page/Section

Initial Notification Contact — Page/Section

- ☐ Clark Kent
- ☐ Lois Lane
- ☐ IMT Members

Contact	Title	Office Phone	Home Phone	Mobile Phone
Herbert Hoover				
Betty Crocker				
Pillsbury Doughboy				
Etc., etc., etc.				

☐ **Assembly** (in the event of building evacuation) — Page/Section

- ☐ Pick Assembly Point and Provide Instructions
  - ☐ Account for all Personnel

☐ **Conduct a Preliminary Assessment.** Determine:

- ☐ Status of Emergency Response
- ☐ Incident Analysis
- ☐ Injuries and Fatalities
- ☐ Areas Affected
- ☐ Security
- ☐ Building Access
- ☐ Status of the Following:
- ☐ Facilities

These example checklists are provided by permission from Chuck Walts, CBCP, CRP, Senior Consultant, SunGard Planning Solutions, Inc.

- ☐ Power
- ☐ Utilities
- ☐ HVAC
- ☐ Environmental Conditions
- ☐ Data Center
- ☐ Voice Communications
- ☐ Data Communication

☐ **Designate Command Center** (at least 2 possibilities are recommended)
- ☐ On Premise (if the building is habitable)
  - ☐ Hogan/Watson Bldg., 3rd Floor Conference Room, Telephone 808-955-6811
- ☐ Off Premise (if access to the main offices is denied)
  - ☐ Warehouse at 12th and Main
  - ☐ Village Inn Restaurant

☐ **Conduct Situation Briefing** (as appropriate)

☐ **Assess Damage**
- ☐ Form Team
- ☐ Damage Assessment Team Briefing
- ☐ Assess Damage
  - ☐ Document Damage with Video Recorder, Camera, and Forms
- ☐ Analyze Damage and Impact
  - ☐ Identify Salvageable Equipment

☐ **Conduct Damage Assessment Brief/Debriefing**
- ☐ Provide instructions (policy/procedure) for dealing with the press/media

☐ **Develop a Consolidated Action Plan**
- ☐ Review Planned Recovery Strategy
- ☐ Review Operational Status
- ☐ Assess Business Impact
- ☐ Develop Recovery Recommendation
  - ☐ Review Maximum Acceptable Outage Duration
  - ☐ Review Recovery Timeline(s) and Assumptions
- ☐ Finalize Recovery Recommendation
- ☐ Review Disaster Declaration Criteria
- ☐ Formulate a Disaster Declaration Recommendation
- ☐ Brief Executive Management
  - ☐ Obtain Disaster Declaration Approval
  - ☐ Obtain/Develop Corporate Media Statement
- ☐ Disaster Decision
  - ☐ If Declaration = No
    - ☐ Recover in place, using locally available resources
  - ☐ If Declaration = Yes
    - ☐ Implement Disaster Recovery Plan and Consolidated Action Plan
    - ☐ Direct Systems and Operations Team Leader to Notify Hotsite

These example checklists are provided by permission from Chuck Walts, CBCP, CRP, Senior Consultant, SunGard Planning Solutions, Inc.

- ☐ **Mobilize Recovery Teams**
  - ☐ Direct Team Leaders to: Call, Assemble and Brief Functional Recovery Team Members
- ☐ **IMT Planning Continues**
- ☐ **Activate Support Personnel (as appropriate)**
  For example:
  - ☐ Human Resources [name]
  - ☐ Finance and Purchasing [name]
  - ☐ Legal [name]
  - ☐ Office Services (Mailroom, Shipping/Receiving)
  - ☐ Records Management
  - ☐ Distribution
  - ☐ Travel
- ☐ **Travel**
  - ☐ Check Travel (Airline) Schedules
  - ☐ Make Travel Arrangement/Reservations
  - ☐ Deploy Teams to Alternate Facilities (as appropriate)
- ☐ **Teams: Implement Functional Recovery Plans**
- ☐ **Operate In Crises Mode**
- ☐ **Coordinate Recovery Actions**
  - ☐ Status Reports
  - ☐ Periodic Briefings (TBD)
- ☐ **Initiate Salvage and Site Restoration (as appropriate)**
- ☐ **Return Home/Transition Planning**
- ☐ **Conduct a Post-Incident Review**
  - ☐ Review All Activity Logs
  - ☐ Debrief Team Personnel
  - ☐ Document "Lessons Learned"
  - ☐ Prepare an After Action Report
- ☐ **Update Disaster Recovery Plans**

Recovery Check List (Systems and Operations)

Action *Reference*

EVENT OCCURRENCE

- ☐ **Incident Detection and Notification**
- ☐ **Event Recognition and Incident Reporting**
- ☐ **Emergency Response, Building Evacuation, and Assembly** (as required)
  - ☐ Assemble on-duty personnel at the designated assembly area (as appropriate)
  - ☐ Account for on-duty personnel (as appropriate)

These example checklists are provided by permission from Chuck Walts, CBCP, CRP, Senior Consultant, SunGard Planning Solutions, Inc.

- ☐ **Provide Instructions to Assembled Personnel** (as appropriate)
  - ☐ Provide support to the incident management team (as required)

Team Leader

- ☐ **Report to Designated Location** (Crisis Management Center)
- ☐ **Participate in IMT Briefing**
- ☐ **Alert Hotsite** (as appropriate)
- ☐ **Alert Off-site Storage Facility Maintaining the Backup Tapes**
  808/ ___ - _____
- ☐ **Participate in Damage Assessment** (Mobilize Selected Team Members, as required)
- ☐ **Attend Damage Assessment Briefing**
- ☐ **Participate in the Consolidated Action Plan Development**
- ☐ **Disaster Decision**
  - ☐ If Declaration = NO
    - ☐ Execute Standard Operational Corrections (On site)
  - ☐ If Declaration = YES
    - ☐ Make Disaster Declaration to Hotsite
    - ☐ Review Recovery Configuration (Equipment/Facility) with Hotsite
    - ☐ Confirm Equipment Availability
    - ☐ Instruct Hotsite to Load Appropriate Operating System
- ☐ **Mobilize Subordinate Functional Recovery Team Leaders**
  - ☐ Systems and Operations
  - ☐ Applications
  - ☐ Network/Communications
  - ☐ Voice Communications

Functional Team Leaders

- ☐ **Call, Assemble, and Brief Team Members**
  - ☐ Make Team Member Assignments
  - ☐ Coordinate Travel Arrangements with the Incident Manager/IMT
  - ☐ Retrieve, Inventory, Verify, and Ship or Pack Backup Tapes
  - ☐ Dispatch Appropriate Team Members to Alternate Facilities (as appropriate)

Contact	Title	Office Phone	Home Phone	Mobile
Bruce Willis	Team Leader			
Sharon Stone	Alternate			
Sylvester Stallone	Member			
Etc., etc., etc.	Member			

- ☐ **Participate in Salvage and Clean-up** (as required)

These example checklists are provided by permission from Chuck Walts, CBCP, CRP, Senior Consultant, SunGard Planning Solutions, Inc.

- ☐ **Conduct Secondary Notifications**
  - ☐ Corporate
    - ☐ [name/phone]
    - ☐ [name/phone]
    - ☐ [name/phone]
  - ☐ Vendors/Suppliers
    - ☐ [name/phone]
    - ☐ [name/phone]
    - ☐ [name/phone]
  - ☐ Key Users
    - ☐ [name/phone]
    - ☐ [name/phone]
    - ☐ [name/phone]
- ☐ Initiate Technical Environment Recovery Procedures at the Alternate Facility
  - ☐ Receive, Inventory, and Check Equipment and Backup Tapes
  - ☐ Install Operating System Using Backup Tapes
  - ☐ Restore Applications and Data from Backup Software
  - ☐ Restore Applications Development Machine
  - ☐ Conduct System Test
  - ☐ Synchronize the Data
  - ☐ Notify Users
    - ☐ Conduct User Acceptance Test(s)
    - ☐ Obtain User Acceptance
  - ☐ Schedule "Catch up" Input of Accumulated Work
  - ☐ Resume Production Processing
- ☐ **Establish a New Tape Library**
- ☐ **Operate in Crisis Mode**
- ☐ **Implement New Backup Procedures**
- ☐ **Assist in Site Restoration**
- ☐ **Assist in Return Home Plan Development**
- ☐ **Transition from Crisis Mode to Home Site Operations**
  - ☐ Conduct a Full System Backup
  - ☐ Ship Backup Tapes to the Home Site
  - ☐ Deploy Personnel from the Alternate Site to the New Home Site
  - ☐ Inspect/Accept New Site
  - ☐ Install Equipment/Inspect New Equipment
  - ☐ Install Operating Systems
  - ☐ Restore Applications and Data from Backup Software
  - ☐ Conduct System Tests
  - ☐ Notify Users
    - ☐ Conduct User Acceptance Test(s)
    - ☐ Obtain User Acceptance
  - ☐ Begin Production

These example checklists are provided by permission from Chuck Walts, CBCP, CRP, Senior Consultant, SunGard Planning Solutions, Inc.

- ☐ **Return to "Business as Usual"**
  - ☐ Conduct a Post-Incident Review
  - ☐ Review All Activity Logs
  - ☐ Debrief Team Personnel
  - ☐ Document "Lessons Learned"
  - ☐ Prepare an After Action Report
- ☐ **Update Disaster Recovery Plans**

These example checklists are provided by permission from Chuck Walts, CBCP, CRP, Senior Consultant, SunGard Planning Solutions, Inc.

APPENDIX 13

Physical Facility Study Questionnaire

Physical Facility Study Questionnaire	Yes	No	Comment	Recommendation
Have all overhead and under floor steam or water pipes been eliminated except for fire sprinklers or machine room requirements?				
Are electrical outlets under raised floor waterproof?				
Do you have water sensors under the raised floor?				
Are all exterior doors and windows water proof?				
Do adjacent areas (restrooms, janitorial rooms, etc) have drainage to prevent overflow into the computer room?				
Is paper stock stored in a water-resistant area?				
Are large waterproof covers available to cover equipment for quick emergency water protection?				
Are openings sealed from upper floor or roof?				
Is computer located under rooftop cooling towers?				
Do you have drainage in computer room?				
Is there a flood control pump for below grade?				
Do you have a roof heating system to melt snow?				
Will the loss of water (or water pressure) halt the operations of your air conditioning?				
Will the loss of water (or water pressure) halt the operations of your water-cooled equipment?				

Physical Facility Study Questionnaire	Yes	No	Comment	Recommendation
Will the loss of water (or water pressure) halt the operations of your fire-fighting equipment?				
Is the building housing the computer constructed of fire resistant and non-combustible material?				
Are combustible materials such as paper and other supplies stored outside the computer room?				
Are tapes and disks stored outside of the computer area?				
Do you have a rated fireproof safe in the computer room for critical file storage?				
Are fire drills practiced periodically and individuals assigned specific responsibilities in case of fire?				
Are emergency phone numbers posted for fire, police, doctors, and hospitals?				
Are both the computer room and tape library protected from fire by use of overhead sprinklers, stand pipe hose, carbon dioxide or halogenated agent?				
Are smoke detectors installed under raised floor and in ceiling?				
Are the detectors installed in the air conditioning system to shut down the fans or switch the system to smoke venting operation?				
Are smoke detectors serviced and tested on a scheduled basis?				
Do you have enunciator panels to assist in quickly locating fire or smoke in unexposed areas?				
Are floor tile removers readily available to expose fire or smoke under raised flooring?				
Are hand extinguishers strategically located around the area with location markers visible over tall computer room equipment?				

Physical Facility Study Questionnaire	Yes	No	Comment	Recommendation
Have employees been instructed on how to use hand extinguishers?				
Is smoking permitted in the computer or tape library area?				
Do employees know the location of the sprinkler shut-off valve and the halon abort switch?				
Are furniture and fixtures made of non-combustible materials?				
Are wastebaskets of metal material with fire retardant tops?				
Do you have emergency lighting in stairwells and corridors for the evacuation of personnel?				
Do you have emergency lighting in the computer area?				
Does the fire alarm sound locally?				
Does the fire alarm sound at the guard station?				
Does the fire alarm sound at the police and fire departments?				
Are there enough audible alarms to alert all personnel?				
Are watchmen schooled as to what to do if a fire occurs during non-working hours?				
In case of fire, would access to the computer area be restricted because of an electrically controlled system?				
Do you have fire dampers in the air ducts?				
Is the air conditioning system dedicated to the computer area?				
Is remote air conditioning equipment secured?				
Are air intakes located above street or protected from contamination?				
Is backup air conditioning by use of a second compressor or chilled water available?				
Are compressor and related air conditioning equipment serviced on a regular schedule?				

Physical Facility Study Questionnaire	Yes	No	Comment	Recommendation
Are air conditioning complete with humidity control?				
Are air temperature and humidity in the computer environment recorded?				
Are building engineers sensitive to the quick response required of computer operations?				
Is air conditioning alarmed in the event of failure?				
Are ducts secured to prevent entry or bombing?				
Do you require uninterrupted power because of the nature of your business?				
If your system requires motor generators, do you have backup?				
Have you checked your local power supply as to reliability?				
Have you monitored your power source with recorders to assure no electrical transients?				
In the event of power failure, do you have emergency electrical power available?				
Is emergency electrical power tested at regular intervals?				
Are power operated doors and fire alarm systems provided with emergency power?				
Do you have lighting arrestors?				
Do you have emergency power-off switches at all exits and within the computer center?				
Does emergency power-off also shut down the air conditioning/heating?				
Are emergency power-off switches protected from accidental activation?				
Is a current copy of your cabling/electrical schematics stored off-site?				
Are intrusion detection devices operational during a power failure?				

Physical Facility Study Questionnaire	Yes	No	Comment	Recommendation
Are intrusion detection devices inspected and tested regularly?				
Is under floor kept clean of dust and dirt?				
Is eating and drinking permitted in the computer room?				
Is equipment kept free of dust and dirt inside and out?				
Is the computer room cleaned on a regular schedule?				
Are employees held responsible for a clean working environment?				
Does management or supervision inspect areas for adherence to good housekeeping?				
Do you have a scheduled removal of empty paper boxes, waste paper and trash?				
Do you display the location of your computer services area?				
Is the computer area visible from the outside of the building?				
If the computer area is visible to the general public, are windows of non-breakable material?				
If there are windows to the computer area that are made of non-breakable material, is the fire department aware that the windows are non-breakable in the event of a fire?				
Is the installation located in a high-crime area?				
Would you consider your company vulnerable to vandalism or a target because of the nature of your business?				
Do you have a 24-hour guard service?				
Do you have a 24-hour guard service for all entrances?				
Do you have a 24-hour guard service for the computer area only?				
Do you use TV cameras in the computer area?				

Physical Facility Study Questionnaire	Yes	No	Comment	Recommendation
Is control of access to the computer area adequate to allow only authorized personnel?				
Are the number of doors leading into the computer area kept to a minimum?				
Do you monitor the status of emergency exits?				
Are doors to the computer area locked at all times?				
Is access to the computer area controlled by use of key, magnetic card, or cipher lock?				
Are access methods changed at regular intervals or after termination of an employee?				
Are dismissed computer environment employees removed immediately and necessary guard personnel notified?				
Is your center alarmed to notify of intrusion?				
Do you have a silent alarm to notify guard personnel of security violations?				
Are security personnel notified of employees permitted access during non-working hours?				
Do company employees escort visiting personnel while in secure areas?				
Are all personnel identified by badge when in the computer area?				
Are visitors in the computer center identified by distinct badges?				
Are operating personnel trained to challenge strangers without proper identification badges?				
Is physical access to the computer room restricted to authorized personnel in accordance with an enforced written policy?				
Is physical access to the computer room restricted to authorized personnel, but with no written policy?				

Physical Facility Study Questionnaire	Yes	No	Comment	Recommendation
Is physical access to the computer room unrestricted?				

If access is restricted, indicate the degree of access to the computer room for each of the following.

	Not Permitted	Permitted Under Special Conditions	Unlimited Access
General Public			
Date Preparation			
Disbursement Personnel			
Auditors			
Consultants			
System Analysts			
Application Programmers			
System Programmers			
Media Librarians			
Control Clerks			
Maintenance Personnel			
Engineers or Customer Engineers			
Other (describe)			
Other–Custodial Supervisor			
Other–Custodians			

APPENDIX 14

Support Reference List

The Support Reference List should include the current name, telephone, location, and functional area of contacts in the following areas:

Business Continuity Planning

Computer Security

Risk Management

Offsite/Vital Records Storage

Offsite Tape Storage

Location 1	Contact	xxx-xxx-xxxx	Iron Mountain	xxx-xxx-xxxx
Location 2	ditto			
Location 3	ditto			
Location 4	ditto			

Replacement of PC Hardware/Software

Site/Space Planning

Telecommunications

Etc.

Business Process Owner Survey

1. Name of Process: _____

   Owner: _____ Phone Number: _____

   Location: _____ Division: _____

   Contact Name: _____ Phone Number: _____

2. Is this process VITAL? Yes __ No __
   If **No**, the remainder of this survey need not be completed.

3. What INTERNAL Computing Applications provide critical support to this vital business process?

Application Name	Owner Name & Phone	Location(s)**
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

4. What other service suppliers (e.g., Mailroom, Distributing, Office systems/Services, LAB, Manufacturing, Vendors, Contractors, etc.) provide critical support to this process?

Organization Name	Contact Name & Phone	Location(s)**
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

5. Name of person completing survey _____ Date _____

** Location = The physical location(s) at which the application/function is processed/performed.

Contributing information to this example comes from Eastman Kodak Company and Texaco, Inc.
Any use or reproduction of this example should include this statement of credits

APPENDIX 16

Phone System Recovery "Hit List"

1. What level of service should be maintained during a disaster?

   Internally and externally in the event of a community disaster?

2. What happens in the event of evacuation? Will there be a requirement for continuous service?

3. What happens if there is a cable cut? Are resources automatically rerouted or could a cable cut on campus cause complete or partial outage?

4. Is there a redundant path?

5. What functional areas are considered critical requiring complete communications functionality, areas requiring partial communications functionality and areas that may require minimum communication functionality?

6. Where will calls be diverted for ISDN, digital and analog lines?

7. Are policies and procedures in place to process the incoming caller professionally and with timely information?

8. How will the organization communicate internally?

9. Where will the help desks or command centers be located and are there resources available to accommodate additional voice and data communication?

10. Is the data center sufficiently backed up with redundancy for critical business applications?

11. Are policies and procedures in place for periodical disaster drills?

12. Do benchmarks measure the success of the drill?

13. What happens if there is only a partial PBX failure, but the outages effect critical care areas within a hospital environment ?

14. What policies and procedures are in place to support the failure ?

Contributing information to this example comes from *BINOMIAL DRP NEWSLETTER,* April 4, 1999.

Contributing information to this example comes from *BINOMIAL DRP NEWSLETTER,* April 4, 1999.

Glossary

ABC Fire Extinguisher: Chemically-based devices used to eliminate ordinary combustible, flammable liquid, and electrical fires.

Activation: When all or a portion of the recovery plan has been put into motion.

Alert: Notification that a disaster situation has occurred—stand by for possible activation of disaster recovery plan.

Alternate Site: A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster. *Similar Terms: alternate processing facility, alternate office facility, alternate communication facility.*

Application Recovery: The component of disaster recovery dealing specifically with the restoration of business system software and data after the processing platform has been restored or replaced. *Similar Terms: business system recovery.*

Assumptions: Basic understandings about unknown disaster situations that the disaster recovery plan is based on.

Back Office Location: An office or building used by the organization to conduct support activities that is not located within an organization's headquarters or main location.

Backlog Trap: The effect on the business of a backlog of work that accumulates when a system or process is unavailable for a long period—a backlog that may take a considerable length of time to reduce.

Backup Agreements: A contract to provide a service which includes the method of performance, the fees, the duration, the services provided, and the extent of security and confidentiality maintained.

Backup Position Listing: A list of alternative personnel who can fill a recovery team position when the primary person is not available.

Backup Power: Generally diesel generators used to provide sufficient power to operate equipment normally when commercial power fails.

Backup Strategy: Alternative operating method (i.e., platform, location, etc.) for facilities and systems operations in the event of a disaster. *See also* Recovery Strategy.

Business As Usual: Operating under normal conditions, i.e., without any significant interruptions of operations as a result of a disaster.

Business Continuity Planning (BCP): An all encompassing, "umbrella" term covering both disaster recovery planning and business resumption planning. *See also* Disaster Recovery Planning and Business Resumption Planning.

Business Function: The most elementary activities, e.g., calculating gross pay, updating job descriptions, matching invoices to receiving reports.

Business Impact Analysis (BIA): The process of analyzing all business functions and the effect that a specific disaster may have upon them.

Business Interruption: Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at a corporate location.

Business Interruption Costs: The costs or lost revenue associated with an interruption in normal business operations.

Business Recovery Coordinator: *See also* Disaster Recovery Coordinator.

Business Recovery Plan: A document containing corporate-wide policies and test-validated procedures and action instructions developed specifically for use in restoring company operations in the event of a declared disaster.

Business Recovery Planning: *See also* Business Continuity Planning, Disaster Recovery Planning, Business Resumption Planning, Contingency Planning.

Business Recovery Process: The common critical path that all companies follow during a recovery effort. There are major nodes along the path that are followed regardless of the organization. The process has seven stages:

1. Immediate response,
2. Environmental restoration,
3. Functional restoration,
4. Data synchronization,
5. Restore business functions,
6. Interim site,
7. Return home.

Business Recovery Team: A group of individuals responsible for maintaining and coordinating the recovery process. *See also* Disaster Recovery Team. *Similar Terms: recovery team.*

Business Recovery Planning (BRP): A "near synonym" for contingency planning. It implies that the plan includes the tasks required to take the organization from the immediate aftermath of a disaster through the return to, or resumption of normal operations. *See also* Disaster Recovery Planning.

Business Unit: Any logical organizational element of a company, agency, or other entity. Contingency plan development can be organized by business unit to define manageable sized organizations to address in a single plan. Business units may reflect specific business functions, a defined section of the organizational chart, the domain of a manager, or some other criteria that provides a definition of scope. The data center is one of the business units in the organization.

Business Unit Recovery: The component of disaster recovery which deals specifically with the relocation of key organization personnel in the event of a disaster, and the provision of essential records, equipment supplies, work space, communication facilities, computer processing capability, etc. *Similar Terms: work group recovery.*

Certified Business Continuity Planner (CBCP): CBCPs are certified by the Disaster Recovery Institute, a not-for-profit corporation that promotes credibility and

professionalism in the disaster recovery industry. This certification originally was known as Certified Disaster Recovery Planner (CDRP).

Checklist Test: A method used to test a completed disaster recovery plan. This test is used to determine if the information, such as phone numbers, manuals, equipment, etc., in the plan is accurate and current.

Cold Site: An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Cold sites have many variations depending on their communication facilities, UPS systems, and mobility. Plans employing a cold site provide a time period when teams procure and install equipment prior to the need to use the facility. *See also* Portable Shell, Uninterruptible Power Supply. *Similar Terms: shell-site, backup site, recovery site, alternate site.*

Command and/or Control Center: A centrally located facility having adequate phone lines to begin recovery operations. Typically it is a temporary facility used by the management team to begin coordinating the recovery process and used until the alternate sites are functional. *Similar Term: emergency operating center.*

Communications Failure: An unplanned interruption in electronic communication between a terminal and a computer processor, or between processors, as a result of a failure of any of the hardware, software, or telecommunications components comprising the link. *See also* Network Outage.

Communications Recovery: The component of disaster recovery that deals with the restoration or rerouting of an organization's telecommunication network, or its components, in the event of loss. *Similar Terms: telecommunication recovery, data communications recovery.*

Computer Recovery Team: A group of individuals responsible for assessing damage to the original system, processing data in the interim, and setting up the new system.

Consortium Agreement: An agreement made by a group of organizations to share processing facilities and/or office facilities, if one member of the group suffers a disaster. *Similar Term: reciprocal agreement.*

Contingency Plan: A predefined collection of procedures and documentation designed to assist an organization to respond to any of a set of disasters, disruptions, or emergencies. The plan provides a mechanism for management and employees to use routine, calm periods of time to carefully consider what actions should be taken under emergency conditions. A contingency plan should contain and describe sufficient management thought and preplanning such that nay employee can implement specific direction guidance of management in an emergency, whether or not the manager is present. *See also* Disaster Recovery Plan.

Contingency Planning: The process of establishing, in advance, strategies and procedures to minimize disruptions of service to an organization and its customers, minimize financial loss, and assure the timely resumption of critical business functions in the event of an unforeseen or unexpected event, disaster, or other interruption. The process and act of planning for contingencies. *See also* Disaster Recovery Planning.

Continuous Availability Services: Data processing disaster recovery services that provide up-to-the-minute recovery capability. Generally, these services involve sophisticated telecommunications networks to capture data continuously during normal operations to prevent loss of any transactions.

Cooperative Hot Sites: A hot site owned by a group of organizations that is available to a group member should a disaster strike. *See also* Hot Site.

Crate and Ship: A strategy for providing alternate processing capability in a disaster, via contractual arrangements with an equipment supplier to ship replacement hardware within a specified time period. *Similar Terms: guaranteed replacement, quick ship*.

Crisis: A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate.

Crisis Management: The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.

Crisis Simulation: The process of testing an organization's ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

Critical Business Functions: Vital business functions without which an organization cannot long operate. If a critical business function is non-operational, the organization could suffer serious legal, financial, goodwill, or other serious losses or penalties.

Critical Records: Records or documents, which, if damaged or destroyed, would cause considerable, inconvenience and/or require replacement or recreation at considerable expense.

Damage Assessment: The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc., and determining what can be salvaged or restored and what must be replaced.

Data Backup: The process of copying the essential elements of a data processing function, programs, data, data bases, procedures, documentation, etc. Data backup to support any recovery effort must include a storage strategy that physically separates the backup data from the original data, such that there is an absolutely minimal chance that the same event could destroy both copies. Off-site storage in a secure environment is the generally accepted solution.

Data Base Shadowing: A data backup strategy in which a full copy of the user's data base is maintained at a remote data center, often a vendor's facility. "Writes" to the primary data base also trigger a transmission and a similar "write" to the remote data base. A disaster or interruption at the primary data center may also impact the data base. A successful recovery, very near to the point of failure, is possible using the shadow data base.

Data Synchronization: A process during recovery of a data system. The conditions that existed at a specific point in time prior to the interruption must be reconstructed such that the processing functions can restart. Multiple data bases or copies of data must be restored to the same or a consistent point in time. Unsuccessful synchronization of data

may result in processing functions restarting using data bases from multiple points in time. The products of the processing functions may not reflect an accurate picture and critical functions may produce serious errors.

Data Center Recovery: The component of disaster recovery that deals with the restoration, at an alternate location, of data center services and computer processing capabilities. *Similar Term: mainframe recovery*.

Data Center Relocation: The relocation of an organization's entire data processing operation.

Dedicated Line: A pre-established point-to-point communication link between computer terminals and a computer processor, or between distributed processors, which does not require dial-up access.

Declaration: A formal statement that a state of disaster exists.

Declaration Fee: A one-time fee, charged by an alternate facility provider, to a customer who declares a disaster. *Note:* Some recovery vendors apply the declaration fee against the first few days of recovery. *Similar Terms: notification fee*.

Departmental Recovery Team: A group of individuals responsible for performing recovery procedures specific to their department.

Dial Backup: The use of dial-up communication lines as a backup to dedicated lines.

Dial-Up Line: A communication link between computer terminals and a computer processor, which is established on demand by dialing a specific telephone number.

Disaster: Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time. *Similar Terms: business interruption, outage, catastrophe*.

Disaster Management: The function of controlling the activities of an organization taken in response to a disaster situation. The functions of an emergency management team in an emergency operating center are functions of disaster management. Disaster management continues through the recovery stages until normal business function resumes.

Disaster Prevention: Measures employed to prevent, detect, or contain incidents which, if unchecked, could result in disaster.

Disaster Prevention Checklist: A questionnaire used to assess preventative measures in areas of operations such as overall security, software, data files, data entry reports, microcomputers, and personnel.

Disaster Recovery: The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.

Disaster Recovery Administrator: The individual responsible for documenting recovery activities and tracking recovery progress.

Disaster Recovery Coordinator: The disaster recovery coordinator may be responsible for overall recovery of an organization or unit(s). *See also* Business Recovery Coordinator.

Disaster Recovery Period: The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.

Disaster Recovery Plan: The document that defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

Disaster Recovery Planning: The technological aspect of business continuity planning. The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster. *Similar Terms: contingency planning, business resumption planning, corporate contingency planning, business interruption planning, disaster preparedness.*

Disaster Recovery Software: An application program developed to assist an organization in writing a comprehensive disaster recovery plan.

Disaster Recovery Life Cycle: Consists of
(1) Normal Operations—the period of time before a disaster occurs;
(2) Emergency Response—the hours or days immediately following a disaster;
(3) Interim Processing—the period of time from the occurrence of a disaster until temporary operations are restored; and,
(4) Restoration—the time when operations return to normal.

Disaster Recovery Teams: A structured group of teams ready to take control of the recovery operations if a disaster should occur. *See also* Business Recovery Teams.

Distributed Processing: The use of computers at various locations, typically interconnected via communication links, for the purpose of data access and/or transfer.

Downloading: Connecting to another computer and retrieving a copy of a program or file from that computer.

Due Diligence: The practice of gathering the necessary information on actual or potential risks so that a well formulated decision may be reached regarding the potential for financial loss.

Electronic Vaulting: Transfer of data to an offsite storage facility via a communication link rather than via portable media. Typically used for batch/journaled updates to critical files to supplement full backups taken periodically.

Emergency: A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.

Emergency Management: The discipline which ensures an organization, or community's readiness to respond to an emergency in a coordinated, timely, and effective manner. *Similar Terms: crisis management, disaster management, emergency preparedness.*

Emergency Preparedness: The part of the overall contingency plan or related activities that occurs prior to the disaster or event and is focused on the safety of personnel and the protection of critical assets. The contingency plan may reference the emergency preparedness program of the safety office or some other responsible organization.

Emergency Procedures: A plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.

Emergency Response Planning: The portion of contingency planning that is focused on the immediate aftermath of a disaster or event. Emergency response planning includes the activities required to stabilize a situation and to protect lives and property.

Employee Relief Center (ERC): A predetermined location for employees and their families to obtain food, supplies, financial assistance, etc., in the event of a catastrophic disaster.

Escalation Procedures: The procedures that define the conditions or criteria under which a plan, or a portion of a plan, will be activated. For most incidents, the initial escalation procedures may call for the staff on duty to handle the incident and notify their supervisor. Escalation procedures for a data processing plan with a commercial hot site will include the conditions under which the hot site vendor is to be notified, and identify who is authorized to make the official declaration of an emergency condition that warrants expending company and vendor resources.

Event: An occurrence of something that elicits a response. A circumstance that causes some action to ensue in response to the situation that has occurred. An unexpected event is an exception to the rule and poses a condition or set of conditions which can escalate in severity if an appropriate and timely response does not take place. For the contingency planner, a disaster, interruption, or any other occurrence, which causes the contingency plan to be activated, or considered for activation.

Executive Succession: That part of the contingency plan which defines the order in which agency executives will assume operational control of the agency in the absence of the primary agency head.

Exercise: A test or drill in which actions in the contingency plan are performed or simulated as though responding to an event. It is during the exercise that planners and participants can evaluate whether the planned activities and tasks properly address potential situations.

Exposure: A state of condition of being unprotected or vulnerable to harm or loss. In the business sense, exposure is the condition of having agency assets and/or resources subject to risk.

Extended Outage: A lengthy, unplanned interruption in system availability due to computer hardware or software problems, or communication failures.

Extra Expense Coverage: Insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster.

Facility: A location containing the equipment, supplies, voice, and data communication lines to conduct business under normal conditions. *Similar Terms: primary site, primary processing facility, primary office facility.*

File Backup: The practice of dumping (copying) a file stored on disk or tape to another disk or tape. This is done for protection case the active file gets damaged.

File Recovery: The restoration of computer files using backup copies.

File Server: The central repository of shared files and applications in a computer network (LAN).

Financial Impact: An operating expense that continues following an interruption or disaster, which, as a result of the event, cannot be offset by income and directly affects the financial position of the organization.

Foreign Corrupt Practices Act: An act of Congress mandating that corporate officers and responsible managers ensure the appropriate degree of control to effectively protect organizational assets.

Forward Recovery: The process of recovering a data base to the point of failure by applying active journal or log data to the current backup files of the data base.

Full Recovery Test: An exercise in which all recovery procedures and strategies are tested (as opposed to a partial recovery test.)

Generator: An independent source of power usually fueled by diesel or natural gas.

Halon: A gas used to extinguish fires effective only in closed areas.

Hazard: A dangerous situation or event which may or may not lead to an emergency or a disaster.

Hazardous Material: The term used to identify any material or substance which may pose a threat to health or safety.

Hazardous Material Team (HAZMAT): A team of professionals trained in handling, storage and disposal of hazardous material.

High Priority Tasks: Activities vital to the operation of the organization. Currently being phased out due to environmental concerns. *Similar Term: critical functions.*

Hot Site: An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster. Hot sites may vary in type of facilities offered (such as data processing, communication, or any other critical business functions needing duplication). Location and size of the hot site will be proportional to the equipment and resources needed. *Similar Terms: backup site, recovery site, recovery center, alternate processing site.*

Human Threats: Possible disruptions in operations resulting from human actions (i.e., disgruntled employee, terrorism, etc.).

Impact: Impact is the cost to the enterprise, which may or may not be measured in purely financial terms.

Incident Commander: The person designated to direct and control the activities at the site of an incident.

Incident Command System: An organizational structure used to direct, control and manage a disaster incident. The incident command center and the commander are

located at the scene of the disaster and are responsible for activities in the immediate physical area. There may be another management center in another locations with overall responsibilities for the disaster activities.

Interim Organizational Structure: An alternate organization structure that will be used during recovery from a disaster. This temporary structure will typically streamline chains of command and increase decision-making autonomy.

Interim Processing Guidelines: Procedures which outline how specific activities will be performed until normal processing capability is restored.

Interim Processing Period: The period of time between the occurrence of a disaster and time when normal operations are restored.

Interagency Contingency Planning Regulation: A regulation written and imposed by the Federal Financial Institutions Examination Council concerning the need for financial institutions to maintain a working disaster recovery plan.

Internal Hot Sites: A fully equipped alternate processing site owned and operated by the organization.

Interruption: An outage caused by the failure of one or more communications links with entities outside of the local facility.

Journaling: Keeping a journal. A journal for a computer includes a record of changes made in files, messages transmitted, etc. It can be used to recover previous versions of a file before updates were made, or to reconstruct the updates if an updated file gets damaged.

LAN Recovery: The component of Disaster Recovery which deals specifically with the replacement of LAN equipment in the event of a disaster, and the restoration of essential data and software *Similar Term: client/server recovery*.

Leased Line: Usually synonymous with dedicated line.

Line Rerouting: A service offered by many regional telephone companies allowing the computer center to quickly reroute the network of dedicated lines to a backup site.

Line Voltage Regulators: Also known as surge protectors. These protectors/regulators distribute electricity evenly.

Local Area Network (LAN): Computing equipment, in close proximity to each other, connected to a server which houses software that can be access by the users. This method does not utilize a public carrier. *See also* Wide Area Network (WAN).

Loss: The unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

Loss Reduction: The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction is intended to react to an event and limit its effect. Examples of loss reduction include sprinkler systems, insurance policies, and evacuation procedures.

Mainframe Computer: A high-end computer processor, with related peripheral devices, capable of supporting large volumes of batch processing, high performance on-line transaction processing systems, and extensive data storage and retrieval. *Similar Terms: host computer.*.

Media Transportation Coverage: An insurance policy designed to cover transportation of items to and from an electronic data processing center, the cost of reconstruction and the tracing of lost items. Coverage is usually extended to transportation and dishonesty or collusion by delivery employees.

Magnetic Ink Character Reader (MICR) Equipment: Equipment used to imprint machine readable code. Generally, financial institutions use this equipment to prepare paper data for processing, encoding (imprinting) items such as routing and transit numbers, account numbers and dollar amounts.

Mission: In a government environment, the mission is the organization's reason for existing.

Mitigation: Any measure taken to reduce or eliminate the exposure of assets or resources to long-term risk caused by natural, man-made, or technological hazards. Any measures taken to reduce frequency, magnitude, and intensity of exposure to risk or to minimize the potential impact of a threat.

Mobile Hot Site: A large trailer containing backup equipment and peripheral devices delivered to the scene of the disaster. It is then hooked up to existing communication lines.

Mobilization: The activation of the recovery organization in response to an emergency or disaster declaration.

Modulator Demodulator Unit (MODEM): Device that converts data from analog to digital and back again.

Natural Threats: Events caused by nature causing disruptions to an organization.

Network Architecture: The basic layout of a computer and its attached systems, such as terminals and the paths between them.

Network Outage: An interruption in system availability as a result of a communication failure affecting a network of computer terminals, processors, or workstations.

Node: The name used to designate a part of a network. This may be used to describe one of the links in the network, or a type of link in the network (for example, host node or intercept node).

Nonessential Function/Data: Business activities or information which could be interrupted or unavailable indefinitely without significantly jeopardizing critical functions of an organization.

Nonessential Records: Records or documents which, if irretrievably lost or damaged, will not materially impair the organization's ability to conduct business.

Notification List: A list of key individuals to be contacted, usually in the event of a disaster. Notification lists normally contain phone numbers and addresses, which may be used in the event that telephones are not operational.

Off-Host Processing: A backup mode of operation in which processing can continue throughout a network despite loss of communication with the mainframe computer.

Off-Line Processing: A backup mode of operation in which processing can continue manually or in batch mode if the on-line systems are unavailable.

Off-Site Storage Facility: A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored.

On-Line Systems: An interactive computer system supporting users over a network of computer terminals.

Operating Software: A type of system software supervising and directing all of the other software components plus the computer hardware.

Organization Chart: A diagram representative of the hierarchy of an organization's personnel.

Organization-Wide: A policy or function applicable to the entire organization and not just one single department.

Orphaned Data: The data which describes the actions or transactions which are accomplished via an alternate method during the period between an interruption to the data processing function and the recovery of the data processing functions.

Outage: *See also* Systems Outage.

Outsourcing: The transfer of data processing functions to an independent third party.

Parallel Test: A test of recovery procedures in which the objective is to parallel an actual business cycle.

Peripheral Equipment: Devices connected to a computer processor which perform such auxiliary functions as communications, data storage, printing, etc.

Physical Safeguards: Physical measures taken to prevent a disaster, such as fire suppression systems, alarm systems, power backup and conditioning systems, access control systems, etc.

Platform: A hardware or software architecture of a particular model or family of computers (i.e., IBM, Tandem, HP, etc.)

Plan Maintenance: Periodic and regular review and updating of a contingency plan.

Planning Software: A computer program designed to assist in the development, organization, printing, distribution, and maintenance of contingency plans.

Portable Shell: An environmentally protected and readied structure that can be transported to a disaster site so equipment can be obtained and installed near the original location. *See also* Mobile Hot Site, Relocatable Shell.

Procedural Safeguards: Procedural measures taken to prevent a disaster, such as safety inspections, fire drills, security awareness programs, records retention programs, etc.

Processing Backlog: The documentation of work and processes that were performed by manual or other means during the time that the data center was unavailable.

Readiness Audit: The determination whether the resources for business recovery are currently available.

Reciprocal Agreement: A mutual aid agreement between two departments, divisions, or agencies wherein each agrees to provide backup data processing support to the other in the event of a disaster. These require a substantial degree of hardware and software compatibility between the supporting and supported partners. The supporting partners must have the excess capacity to accommodate the sending partner's most critical applications. These agreements are seldom successful and many auditors to not recognize them as viable disaster recovery strategies.

Record Retention: Storing historical documentation for a set period of time, usually mandated by state and federal law or the Internal Revenue Service.

Recovery Action Plan: The comprehensive set of documented tasks to be carried out during recovery operations.

Recovery Alternative: The method selected to recover the critical business functions following a disaster. In data processing, some possible alternatives would be manual processing, use of service bureaus, or a backup site (hot or cold site). A recovery alternative is usually selected following either a risk analysis, business impact analysis, or both. *Similar Terms: backup site, backup alternative.*

Recovery Capability: This defines all of the components necessary to perform recovery. These components can include a plan, an alternate site, change control process, network rerouting and others.

Recovery Management Team: A group of individuals responsible for directing the development and ongoing maintenance of a disaster recovery plan. Also responsible for declaring a disaster and providing direction during the recovery process.

Recovery Planning Team: A group of individuals appointed to oversee the development and implementation of a disaster recovery plan.

Recovery Point Objective (RPO): The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed.

Recovery Strategy: The method selected by an organization to recover its critical business functions following a disaster. Possible strategies for recovering from an event which degrades or halts scheduled data processing services delivery are:

1. Revert to manual procedures.
2. Temporarily suspend data processing operations to effect recovery on-site.
3. Contract with a service to provide essential data processing operations from that location.
4. Transfer essential data files and applications from off-site storage to a hot-site facility and begin processing from the hot site.

Recovery Team: *See also* Business Recovery Team, Disaster Recovery Team.

Recovery Time: The period from the disaster declaration to the recovery of the critical functions.

Relocatable Shell: *See also* Portable Shell, Mobile Hot Site.

Redundancy: Providing two or more resources to support a single function or activity with the intention that if one resource fails or is interrupted, an alternate resource will immediately begin to perform the function.

Remote Access: The ability to use a computer system, generally a mainframe, from a remote location, generally by common phone lines.

Remote Journaling: The process of recording the product of a computer application in a distant data storage environment, concurrently with the normal recording of the product in the local environment. May be periodic or continuous.

Restoration: The act of returning a piece of equipment or some other resource, to operational status. Commercial service companies provide a restoration service with staff skilled in restoring sensitive equipment or large facilities.

Resumption: The process of planning for and/or implementing the recovery of critical business operations immediately following an interruption or disaster.

Risk: The potential for harm or loss. The chance that an undesirable event will occur.

Risk Analysis/Assessment: The process of identifying and minimizing the exposures to certain threats which a organization may experience.

Qualitative Risk Analysis: The relative measure of risk or asset value by using subjective terms such as low, medium, high, 1-10, not important, very important, etc.

Quantitative Risk Analysis: Using objective statistical data to measure risk, asset value and probability of loss. *Similar Terms:* risk assessment, impact assessment, corporate loss analysis, risk identification, exposure analysis, exposure assessment.

Risk Management: The discipline which ensures that an organization does not assume an unacceptable level of risk.

Salvage and Restoration: The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc., following a disaster.

Salvage Procedures: Specified procedures to be activated if equipment or a facility should suffer any destruction.

Sample Plan: A generic disaster recovery plan that can be tailored to fit a particular organization.

Satellite Communication: Data communications via satellite. For geographically dispersed organizations, may be viable alternative to ground-based communications in the event of a disaster.

Scenario: A predefined set of events and conditions which describe an interruption, disruption or disaster related to some aspect(s) of an organization's business for purposes of exercising a recovery plan(s).

Scope: Predefined areas of operation for which a disaster recovery plan is developed.

Secondary Disasters: Disasters which occur as collateral events associated with a primary disaster. Earthquakes are primary disasters which may cause subsequent fires, etc.

Service Bureau (Center): A data processing utility that provides processing capability, normally for specialized processing, such as payroll.

Service Level Agreement (SLA): An agreement between a service provider and service user as to the nature, quality, availability and scope of the service to be provided.

Shadow File Processing: An approach to data backup in which real-time duplicates of critical files are maintained at a remote processing site. *Similar Terms: remote mirroring.*

Simulation Test: A test of recovery procedures under conditions approximating a specific disaster scenario. This may involve designated units of the organization actually ceasing normal operations while exercising their procedures.

Single Point of Failure: An element of a system for which no redundancy exists. A failure of such a component may disable the entire system.

Skills Inventory: A roster of employees that lists their skills that apply to recovery.

Social Impact: Any incident or happening that affects the well-being of a population and which is often not financially quantifiable.

Stand-Alone Processing: Processing, typically on a PC or mid-range computer, which does not require any communication link with a mainframe or other processor.

Stand Down: Formal notification that the alert may be called off or that the state of disaster is over.

Structured Walk-Through Test: Team members walk through the plan to identify and correct weaknesses.

Subscription: Contract commitment providing an organization with the right to utilize a vendor recovery facility for recovery of their mainframe processing capability. Usually requires a subscription fee.

System Downtime: A planned interruption in system availability for scheduled system maintenance.

System Outage: An unplanned interruption in system availability as a result of computer hardware or software problems, or operational problems.

Table-Top Exercise: A type of test of a contingency plan in which actions are not actually performed. Participants read through the steps and procedures of the plan, in sequence, and evaluate the expected effectiveness of the plan the interaction between elements of the plan.

Technical Threats: A disaster causing event that may occur regardless of any human elements.

Temporary Operating Procedures: Predetermined procedures which streamline operations while maintaining an acceptable level of control and auditability during a disaster situation.

Testing: *See also* Exercise.

Test Plan: The recovery plans and procedures that are used in a systems test to ensure viability. A test plan is designed to exercise specific action tasks and procedures that would be encountered in a real disaster. *Similar Term: test script.*

Threat: Threats are events that cause a risk to become a loss. Example: A lightning strike could be the trigger that causes a fire that destroys a facility. Threats include natural phenomena and man-made incidents.

Tolerance Threshold: The maximum period of time which the business can afford to be without a critical function or process.

Uninterruptible Power Supply (UPS): A backup power supply with enough power to allow a safe and orderly shutdown of the central processing unit should there be a disruption or shutdown of electricity.

Uploading: Connecting to another computer and sending a copy of a program or file to that computer. *See also* Downloading.

Useful Records: Records that are helpful but not required on a daily basis for continued operations.

User Contingency Procedures: Manual procedures to be implemented during a computer system outage.

User Preparedness Reviews: Periodic simulations of disaster recovery conditions for the purpose of evaluating how well an individual or department is prepared to cope with disaster conditions.

Vulnerability: The degree to which people, property, resources, and commerce, as well as environmental, social, and cultural activity are susceptible to harm or destruction.

Vital Records: Records or documents, for legal, regulatory, or operational reasons, cannot be irretrievably lost or damaged without materially impairing the organization's ability to conduct business.

Voice Recovery: The restoration of an organization’s voice communications system.

Walk-Through: A type of exercise or plan test. The plan or sections of the plan are reviewed in a systematic manner in which each planned step is discussed and described to ensure appropriateness in that scenario. Effective method to verify coordination between plan elements.

Warm Site: An alternate processing site which is only partially equipped (as compared to hot site, which is fully equipped).

Wide Area Network (WAN): Like a LAN, except that parts of a WAN are geographically dispersed, possible in different cities or even on different continents. Public carriers like the telephone company are included in most WANs; a very large WAN might have its own satellite stations or microwave towers.

Sources and References

Sources Used in the Development of these Guidelines

Arber, Damon. "Auditing Business Recovery Plans," *Disaster Recovery Journal*, Winter 1997.

Business Continuity Journal #20, 1998.

Carlson, Dan, Dayton Hudson Corporation.

Comdisco Disaster Recovery Services, Rosemont, IL.

Devlin, Edward., Emerson, Cole H., Wrobel, Jr., Leo A., *Business Resumption Planning*, Auerbach, RIA Group, New York, 1996.

Disaster Recovery Journal, Editorial Advisory Board, Learning the Terminology Web Site.

Fisher, Patricia A.P., "How to Conduct a Business Impact Analysis," *Disaster Recovery Journal*, Volume 9, Issue 3, Summer 1996 p. 64–68.

Gooding, C., Cuthbertson, G., Smith, C. *Planning for Business Continuity*, Gartner Group, R-980-104, Strategic Analysis Report, October 25, 1996.

Grindler, Gerald W., *Handbook of Information Security*, Auerbach, Chapter 1-4-1.

Harris, Norman L., *Advanced: Concepts & Techniques Business Recovery Planning & Security*, Harris Disaster Recovery Associates, 1996.

Helsing, Cheryl W., "Corporate Contingency Planning: A Blueprint for Survival," Datapro IS38-320, May 1991.

Jackson, Carl B., *Business Continuity Planning: The Need and the Approach*, Datapro Information Services Group, January 1996.

Jones, B. "BIA: The Foundation of Business Continuity Planning," Gartner Group, SPA-890-1244, March 21, 1996.

Jones, B. "Determinants of Business Continuity Expenditure," Gartner Group, KA-890-1246.

Kirsle, John, Federated Mutual Insurance.

Business Recovery Planning: The Who and the What. SSMS 21 21 Nov 95.499, META Group, Inc. Stamford, CT.

Meglathery, Sally "Developing a Business Continuity Plan," *Handbook of Information Security*, Auerbach, Chapter 1-4-2 .

Missing Link Communications, Inc., 8701 Kerry Lane, Springfield, VA.

Northern California Chapter, Association of Contingency Planners, Contingency Planner's Glossary.

Rothstein, Philip Jan, Editor. *Disaster Recovery Testing, Exercising Your Contingency Plan*, Rothstein Associates, Inc. Ossining, New York, 1994.

Risk Management for State Agencies, published by the Texas State Office of Risk Management.

Smith, Kenneth A. "Developing and Testing Business Continuity Plans," *Handbook of Data Center Management*, 1996–97 Yearbook, Auerbach VII-2, S-185 (comparing strategy table).

SunGard Planning Solutions, Wayne, PA.

Toigo, Jon. *Disaster Recovery Planning for Computers and Communication Resources*, John Wiley & Sons, Inc. 1996.

1995 Vulnerability Index: Hidden Risks in Computer-Aided Productivity, Wave Two, A Research Report Prepared for Comdisco, Inc. and Palindrome, Corp. to ICR Survey Research Group, Media, PA.

Walts, C., White, T., Light, J., and Albin, M.A. Workshop on Contingency Planning for State Agencies. December 1995.

Wold, Geoffrey H., "Some Techniques for Business Impact Analysis," Disaster Recovery Journal, Fall 1996. p. 27-33.

Additional References

Texas State Office of Risk Management (SORM) sponsors a one-day orientation session periodically on Contingency Planning for State Agencies.

Contingency Planning and Disaster Recovery: Protecting Your Organization's Resources; Janet G. Butler, Poul Badura.

Fire in the Computer Room, What Now? Disaster Recovery: Preparing for Business Survival; Gregor Neaga, et. al.

LAN: Disaster Prevention and Recovery ; Patrick H. Corrigan.

Disaster Recovery for LANs: A Planning and Action Guide; Regis J. "Bud" Bates.

Disaster Recovery Planning: Networks, Telecommunications and Data Communications (J. Ranade Series on Computer Communications); Regis J. "Bud" Bates.

Periodicals and Hot Links

Disaster Recovery Journal — www.drj.com

Contingency Planning and Management — www.disaster-resource.com

Disaster Resource Guide — www.disaster-resource.com

Business Continuity Institute — www.thebci.org

The Business Continuity Group — www.survive.com

Natural Hazards Center at the University of Colorado, Boulder — www.Colorado.EDU/hazards/

The Disaster Research Center — www.udel.edu/DRC/

DRI International — www.dr.org

The Business Continuity Information Centre — www.business-continuity.com

Listings of documents/papers on mass de-acidification process — palimpsest.stanford.edu/bytopic/massdeac/

National Library of Australia, Disaster Recovery Plan — www.nla.gov.au/policy/disaster.html

Business Continuity Pages for Beginners — www.drj.com/new2dr/newbies.htm

Professional Practices for Business Continuity Practitioners — www.dr.org/ppover.htm

Disaster Recovery Planning: Project Plan Outline, University of Toronto — www.utoronto.ca/security/drp.htm#DRP

Why Bother with Recovery Time? www.bmc.com/products/articles/arxxdb000a.html

Links to other Disaster Recovery Sites — www.binomial.com/

University of Illinois Preparedness and Recovery — www.ag.uiuc.edu/~disaster/prepare.html

Disaster Information Network — www.disaster.net/index.html

202 Links to Sites related to Disaster Recovery — www.woodtech.com/~envirocomnet/

Comparison of Requests for Proposals for Disaster Recovery Services

Network Computing Online — www.networkcomputing.com/1001/1001f1.html

Montana State ISD, Disaster Recovery Background & Disaster Recovery Goals & Objectives — www.mt.gov/isd/planning/disaster/

Disaster Recovery Yellow Pages — www.disasterplan.com/yellowpages/

List of “Small But Critical” and Often Overlooked Planning Items — www.disasterplan.com/yellowpages/Remember.html

Sample Business Continuity Plan, MIT — web.mit.edu/security/www/pubplan.htm

E-mail List Services

BINOMIAL DISASTER RECOVERY WEB-LETTER — majordomo@magmacom.com (DISASTER-RECOVERY)

Disaster Prevention & Recovery Alliance — ListDPRA-REQUEST@INFOMANAGE.COM (listdpra)

Disaster Recovery Journal — www.drj.com/subscription/subindex.html

Disaster-Recovery — majordomo@magnacom.com (DISASTER RECOVERY)

DRP-L — listserv@vm.marist.edu (DRP-L)

LEPC Hazardous Materials Response Planning — listserv@moose.uvm.edu (LEPC your name)

NETS — nets-request@oes.ca.gov

ARMA — listserv@listserv.syr.edu (RECMGMT)

DIR Technology Information Center

The Department of Information Resources offers resources and research assistance, specific to information technology issues, to Texas state agency and university employees, by appointment only. Resources include journals, books, federal and state government publications, CD-ROM databases, and online access to IT advisory services.

Call the Technology Information Center at 512-475-4790 for information or to make an appointment.

Research and Advisory Services

Gartner Group — Established in 1979 by Gideon Gartner, provides multiple services based on specific information technologies.

Giga Information Group — Established in 1995 by Gideon Gartner, offers unified research coverage in a single service known as the Giga Advisory.

META Group — Established in 1989 by Dale Kutnick and Marc Butlein, offers seven core information technology services.

All three research and advisory services are Qualified Information Systems Vendors for the State of Texas. Information about pricing can be obtained by visiting the General Service Commission's web site, www.gsc.state.tx.us/stpurch/qisv.html, or by telephone at 512-463-8889. The Department of Information Resources has negotiated statewide contracts with META Group and Giga Information Group. To inquire about participating in the contract, please contact DIR at 800-464-1215 or 512-305-9713.

Journals

Disaster Recovery Journal. The journal dedicated to business continuity. Published quarterly by Systems Support Inc; St. Louis, MO.

Info Security News. The magazine for the protection of information. Published bimonthly by MIS training Press, Inc; Framingham, MA.

IS Audit and Control Journal. Formerly the EDP Auditor Journal. The journal of the Information Systems Audit and Control Association. Published bimonthly by the Information Systems Audit and Control Association; Rolling Meadows, IL.

Survive! The business continuity magazine. Published quarterly by LLP Ltd; London, UK.

Books

Byrnes, Chris. *Security in Enterprise Computing: A Practical Guide.* (Stamford, CT: META Group, 1997).

Held, Gilbert, ed. *Communications Systems Management.* (Boca Raton, FL: CRC Press LLC, 1999). Focuses on issues in all aspects of managing communication systems. Includes sections on internet security and network disaster recovery.

Krause, Micki and Harold F. Tipton, ed. *Handbook of Information Security Management.* (Boca Raton, FL: CRC Press LLC, 1999). Thirty percent of the topics in the yearly editions of the handbook are newly introduced material. Topics include telecommunication and network security, continuity planning, security management, risk management, and security architecture.

Purba, Sanjiv, ed. *Handbook of Data Management.* (Boca Raton: CRC Press LLC, 1999). Topics included discuss the role of data security and recovery as an enterprise-wide concern.

Rothstein, Philip Jan. *Disaster Recovery Testing.* (New York: Rothstein Associates Inc, 1994).

Umbaugh, Robert E, ed. *Handbook of IS Management.* (Boca Raton: CRC Press LLC, 1999). Intended for the IS manager, this resources includes topics that address setting IS policy for internet security.

Wyzalek, John, ed. *Handbook of Enterprise Operations Management.* (Boca Raton, FL: CRC Press LLC, 1999). Formerly entitled Handbook of Data Center Management, this book focuses on the wide range of systems IT professionals are now faced with in their management roles. Contains sections on computer security and contingency planning.

Electronic Resources

Computer Select. (v. 3.7) [CD-ROM]. (1999). The Gale Group. A collection of articles about the computer and communications industry. Most articles are full text versions from more than 110 industry journals.

Datapro. [CD-ROM]. (1999). Gartner Group. This extensive database provides access to IT management information, industry best practices, and also includes access to product and vendor comparison information.

Auerbach Information Management Service (AIMS). [CD-ROM]. (1999). Auerbach Publications. Provides up-to-date access to information regarding the administration and management of IT resources.