COMMONd
We help organizations do more for less

BUSINESS CONTINUITY 101

Disclaimer

The following project outline is provided solely as a guide. It is only intended to be "one example" of the requirements for a disaster recovery project plan. It is not, by any stretch of the imagination, the only way to set up a project plan.

Program Description

1. Pre-Planning Activities (Project Initiation)
2. Vulnerability Assessment and General Definition of Requirements
3. Business Impact Analysis
4. Detailed Definition of Requirements
5. Plan Development
6. Testing Program
7. Maintenance Program
8. Initial Plan Testing and Plan Implementation

The primary objective of a Business Resumption Plan is to enable your organization to survive a disaster and to reestablish normal business operations. In order to survive a disaster, you must assure that critical operations can resume normal processing within a reasonable time frame. Therefore, the goals of the Business Resumption Plan should be to:

1. Identify weaknesses and implement a disaster prevention program;
2. Minimize the duration of a serious disruption to business operations;
3. Facilitate effective co-ordination of recovery tasks; and
4. Reduce the complexity of the recovery effort.

Historically, the data processing function alone has been assigned the responsibility for providing contingency planning. Frequently, this has led to the development of recovery plans to restore computer resources in a manner that is not fully responsive to the needs of the business supported by those resources.

Contingency planning is a business issue rather than a data processing issue. In today's environment, the effects of a long-term operations outage may have a catastrophic impact financially as well as to public perception of your healthcare entity. The development of a viable recovery strategy must, therefore, be a product not only of the provider's of the organization's data processing, communications and operations center services, but also the users of those services and management personnel who have responsibility for the protection of the organization's assets.

The methodology used to develop the plans, emphasizes the following key points:

1. Providing the management team of Your organization with a comprehensive understanding of the total effort required to develop and maintain an effective recovery plan
2. Obtaining commitment from appropriate management to support and participate in the effort
3. Defining recovery requirements from the perspective of business functions;
4. Documenting the impact of an extended loss to operations and key business functions
5. Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery
6. Selecting project teams that ensure the proper balance required for plan development
7. Developing a contingency plan that is understandable, easy to use and easy to maintain
8. Defining how contingency planning considerations must be integrated into ongoing business planning and system development processes in order for the plan to remain viable over time

The successful and cost effective completion of such a project requires the close cooperation of management from all areas of Information Systems as well as business areas supported by your organization Information Systems. Senior personnel from your organization and user areas must be significantly involved throughout the project for the planning process to be successful.

In closing, it is important to keep in mind that the aim of the planning process is to:

1. Assess existing vulnerabilities
2. Implement disaster avoidance and prevention procedures
3. Develop a comprehensive plan that will enable your organization to react appropriately and in a timely manner if disaster strikes.

Since recovery planning is a very complex and labor intensive process, it therefore requires redirection of valuable technical staff and information processing resources as well as appropriate funding. In order to minimize the impact such an undertaking would have on scarce resources, the project for the development and implementation of disaster recovery and business resumption plans should be part of the organization's normal planning activities.

The proposed project methodology consists of eight separate phases, as described below.

Phase 1 - Pre-Planning Activities (Project Initiation)

Phase 1 is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to: refine the scope of the project and the associated work program; develop project schedules; and identify and address any issues that could have an impact on the delivery and the success of the project.

During this phase a steering committee should be established. The committee should have the overall responsibility for providing direction and guidance to the project team. The committee should also make all decisions related to the recovery planning effort. The project manager should work with the steering committee in finalizing the detailed work plan and developing interview schedules for conducting the security assessment and the Business Impact Analysis.

Two other key deliverables of this phase are: the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the project.

Phase 2 - Vulnerability Assessment and General Definition of Requirements

Security and control within an organization is a continuing concern. It is preferable, from an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase addresses measures to reduce the probability of an occurrence.

This phase will include the following key tasks:

A thorough security assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.

The security assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
Present findings and recommendations resulting from the activities of the security assessment to the steering committee so that corrective actions can be initiated in a timely manner.

Define the scope of the planning effort.

Analyze, recommend and purchase recovery planning and maintenance software required to support the implementation.

Develop a plan framework, assemble project team and conduct awareness sessions.

Phase 3 - Business Impact Assessment (BIA)

A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to: identify critical systems, processes and functions; assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the steering committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

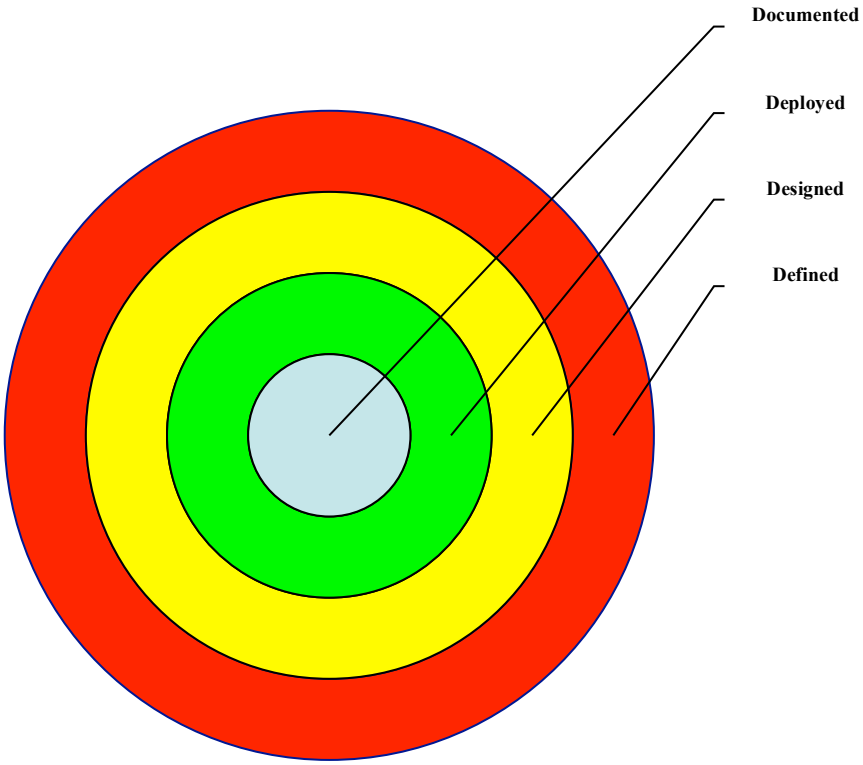
Phase 4 - Detailed Definition of Requirements

During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analyzing alternative recovery strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit. Recovery strategies will be based on short term, intermediate term and long term outages.

Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

Phase 5 - DR Plan Development

During this phase, recovery plan components must have the **4D's**:



Disaster Recovery planner should refer to their organization's business continuity plan and Business Impact Assessment (BIA) which should indicate the key metrics of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for various business processes (such as the process to handle accounts receivables, accounts payable, payroll, eCommerce, customer service, sales, etc.). The metrics specified for the business processes must then be mapped to the underlying IT systems, the skill sets of supporting personnel, the SLA of vendors and their track record(s), and the LAN, WAN, physical, and logical infrastructure that support those processes.

Once the RTO and RPO metrics have been mapped to IT infrastructure, the DR planner can determine the most suitable recovery strategy for each system.

An important note here, however, is that the business ultimately sets the IT budget, and therefore the RTO and RPO metrics need to fit with the available budget. While most business unit heads would like zero data loss and zero time loss, the cost associated with that level of protection may make the desired high availability solutions unpractical.

This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery

services) and the definition of recovery teams, their roles and responsibilities. Recovery standards should also be developed during this phase.

Phase 6 - Testing/Exercising Program

The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.

Phase 7 - Maintenance Program

Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account.

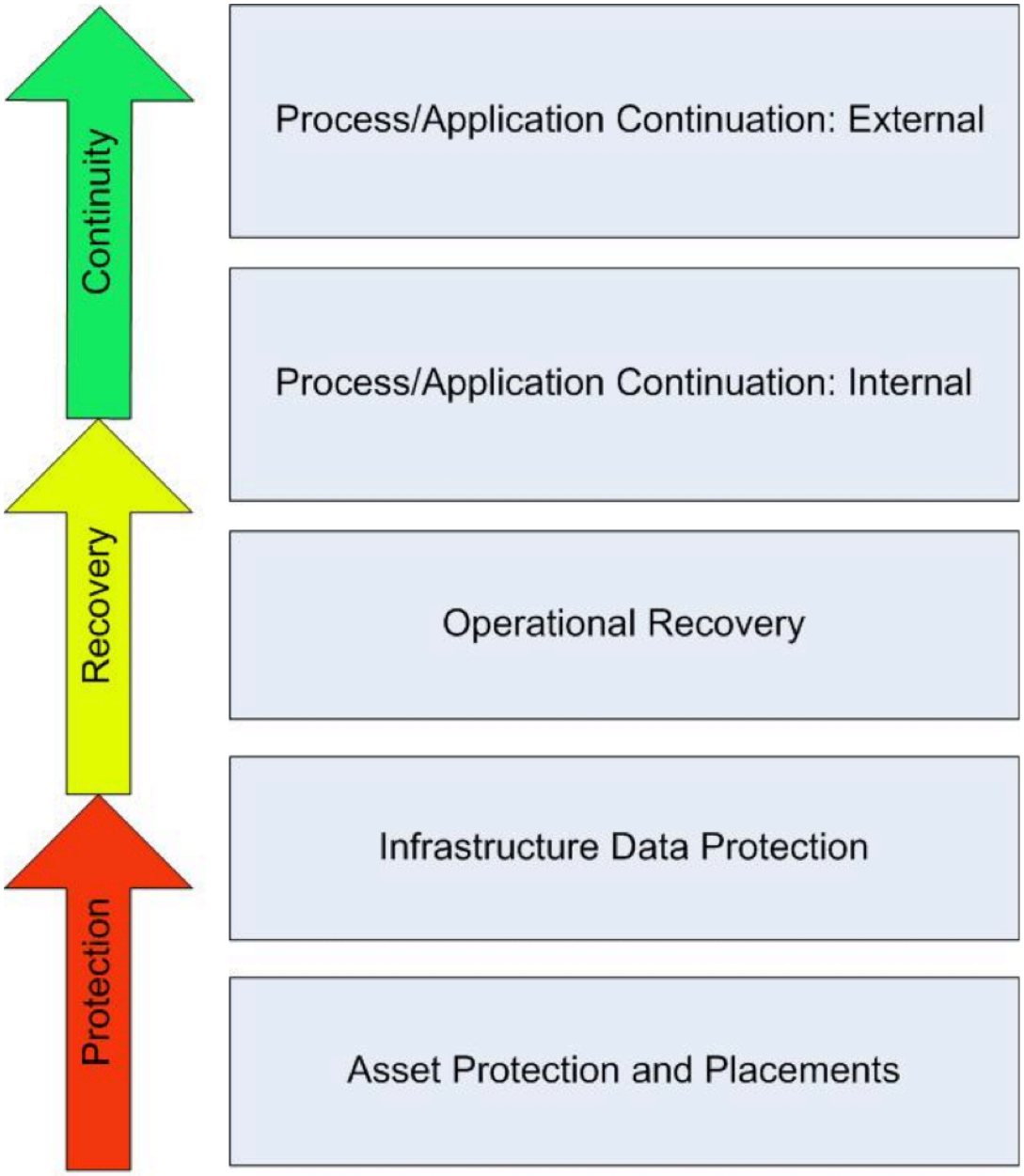
Phase 8 - Initial Plan Testing and Implementation

Once plans are developed, initial tests of the plans are conducted, and any necessary modifications to the plans are made based on an analysis of the test results.

Specific activities of this phase include the following:

1. Defining the test purpose/approach
2. Identifying test teams
3. Structuring the test
4. Conducting the test
5. Analyzing test results
6. Modifying the plans as appropriate

The approach taken to test the plans depends, in large part, on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.


Continuity
Recovery
Protection
Process/Application Continuation: External
Process/Application Continuation: Internal
Operational Recovery
Infrastructure Data Protection
Asset Protection and Placements

Scope and Objective

The primary objective of recovery planning is to enable an organization to survive a disaster and to continue normal business operations. In order to survive, your organization must assure that critical operations can resume/continue normal processing. Throughout the recovery effort, the plan establishes clear lines of authority and prioritizes work efforts. The key objectives of the contingency plan should be to:

Provide for the safety and well-being of people on the premises at the time of a disaster and continue critical business operations:

1. Minimize the duration of a serious disruption to operations and resources (both information processing and other resources)
2. Minimize immediate damage and losses
3. Establish management succession and emergency powers
4. Facilitate effective coordination of recovery tasks
5. Reduce the complexity of the recovery effort
6. Identify critical lines of business and supporting functions

Although statistically, the probability of a major disaster is remote, the consequences of an occurrence could be catastrophic, both in terms of operational impact and public image. Management appreciates the implications of an occurrence; therefore, it should assign on-going responsibility for recovery planning to an employee dedicated to this essential service.

Management must make a decision to undertake a project that satisfies the following objectives:

1. ***Determine vulnerabilities to significant service interruptions in the Data Center and business facilities and define preventive measures that may be taken to minimize the probability and impact of interruptions***
2. ***Identify and analyze the economic, service, public image and other implications of extended service interruptions in the Data Center and other business facilities***
3. ***Determine immediate, intermediate and extended term recovery needs and resource requirements; Identify the alternatives and select the most cost effective approaches for providing backup operations capability and timely service restoration***
4. ***Develop and implement contingency plans that address both immediate and longer-term needs for the Data Center and other business facilities***