White Paper

Published: April 2001 (with revisions)

Business Continuity Planning Description and Framework

Contents

Preface

The terms "Disaster Recovery" and "Business Continuity" are often used interchangeably. They are in fact, different but complementary components of a business's overall recovery and continuity planning. Whereas Disaster Recovery Planning (DRP) is concerned with the recovery of systems and infrastructure components, Business Continuity Planning has a larger scope – namely, the determination of which business components and functions need to be recovered – and those which can be ignored.

This whitepaper will explore several of the key components of a Business Continuity planning effort. It will also provide a high level framework for the creation, implementation, and maintenance of a Business Continuity Plan. The approach presented is one that that has been "field tested" and proven over time. It is also an approach that allows you to get a feel for the capabilities and responsiveness of a service provider before committing to a long-term engagement.

What is BCP?

At the most basic level, <u>Business Continuity Planning (BCP) can be defined as an iterative process that is designed to identify mission critical business functions and enact policies, processes, plans and procedures to ensure the continuation of these functions in the event of an unforeseen event.</u> All activity surrounding the creation, testing, deployment, and maintenance of a BCP can be viewed in terms of this definition.

It is important to keep in mind that each BCP is different – the mission-critical "processes" (not necessarily *application systems*), procedures, and functions captured in the BCP process are those required to run *your specific business*. There may be similarities within industries and from company to company, but each organization is unique, and as such will have a unique BCP. It is always important to keep this in mind – some Business Continuity / Disaster Recovery (BC/DR) service providers will try and shoehorn your organization into a predefined plan. Although this simplifies their job and may reduce your costs, what you are left with may not be what you need when there is a disaster.

Business Continuity (BC) versus Disaster Recovery (DR)

The first challenge of a BC effort is to "get everyone on the same page" by defining and using consistent terminology. Doing so will establish a common vision for the BC team, where everyone understands the overall goal as well as the major steps required to achieve it. <u>It is difficult to agree on what success will look like if there is not a common understanding of the scope of the effort.</u>

Given that, what are the differences between BC and DR?

A DR plan is usually limited in scope to a set of defined IT systems and infrastructure, with the ultimate goal being the complete recovery of those systems and infrastructure within a defined timeframe and with minimal data loss. The DR plan may exclude non-IT business units – such as Accounting, Marketing, Sales, etc., except in terms of recovery of the defined applications used by these business units. The process of determining which IT systems to recover in a DR planning effort is usually driven by the IT department with input from various application owners who may or may not be part of the IT department. This means that the DR requirements definition process may make incorrect assumptions or miss subtleties and/or dependencies that are not hardware or application system dependent (such as document management, retention, and security).

Contrast this with a BC plan that has as its scope the entire enterprise, with the ultimate goal being recovery of mission-critical/core business functions to ensure the survival of the enterprise. <u>The business functions to be recovered in a BC extend beyond IT systems</u> – for example, BC concerns itself not only with the recovery of applications that support sales, but also with the recovery of the related infrastructure (such as office space), supplies (such as marketing materials and manual forms), etc.

The other main difference between a DR and BC concerns the definition of what to recover and what to exclude. Business Continuity requires the definition and determination of response to risk (Risk Analysis and Response), the definition of possible failure areas (a Single Points of Failure, or SPOF analysis), and the determination of the impact of these areas on the business as a whole (Business Impact Analysis, or BIA). This analysis will result in the determination of what business functions are "core" or "mission critical" – these are the business functions that are essential for the survival of the enterprise, and will by necessity be the focus of the BC effort.

Another key area within the scope of the BCP is concerned with data, system, and application dependencies. The failure to identify, plan for, and properly recover systems and processes in light of these dependencies could very well keep a business unit from operating properly. This scenario highlights the importance of these issues, and underscores why they need to be identified early in the BC process and addressed accordingly.

This information logically leads to a question regarding the sequencing of DR and BC efforts, namely, is it better to have a Business Continuity Planning effort as a follow-on effort to a Disaster Recovery Planning project, or should the BCP effort drive a DRP project? Like many of the questions surrounding BC and DR, the answer here is very subjective.

For an enterprise that currently does not possess a DR plan, it will most likely be advantageous to charter a BC effort with the DR effort being directed to address the specific IT requirements defined by the BC effort. However, if an enterprise has a working DR plan or plans, it makes more sense to leverage that knowledge into the creation of the BC plan. In the second case, the integration of the DR plan into the new BC plan is of utmost importance. There is also the chance that portions of the existing DR plan or plans may need to be reworked or become obsolete based on the overall allocation of resources determined by the BC effort.

Do the two teams need to consist of the same group of people? No. But, there does need to be effective communication and coordination between the two teams. Assumptions need to be validated before being acted upon, and nothing should be taken for granted. So, this increases the level of complexity as well as the opportunities for problems. While you may not have a choice, it is important to understand the risks and complexities of this type of approach.

No matter what order the creation of the BCP and DRP are undertaken in, it is necessary to understand that a working DRP is a necessary foundation for a BCP. Put another way, it is possible to have a working DRP without a working BCP – however; it is impossible to have a working BCP without a DRP.

Other Considerations

The following sections detail out additional areas that need to be reviewed and addressed as part of a BC effort. Please note that every BC effort is different, and what works for one organization may not work for all. The key is to determine what works best and is most effective for your organization.

Sponsorship

Unlike a DRP (which can be owned and managed at the department level), the scale, cost, and impact of a true BCP are at the enterprise level and needs to be managed as such. Because of it's logical connection to DRP, many companies BCP plans fall under the responsibility of the IT department – however, since *Business Recovery* comprises many areas that are outside of the scope of the IT department (such as Legal Counsel, Supply Chain, and external agency liaisons), this is often a flawed assumption. Due to these reasons, the use of the CEO, CFO, or other senior manager as the project sponsor/champion is a normal and highly desirable practice.

Best Practices and Regulatory Compliance

A key part of any BC effort is compliance with all pertinent regulatory acts and agencies. For example, all publicly traded companies in the United States are subject to the Sarbanes-Oxley Act (SOX); Healthcare professionals and organizations are subject to HIPAA; Medical Device and Pharmaceutical companies are governed by FDA rules and regulations; and the Banking industry is governed by FDIC rules and regulations.

In addition to these requirements, it is also necessary that a BC effort take into account what are usually referred to as "quasi-regulations". These are industry standards and best practices which, although not required or having the force of regulations, should be followed. Compliance with these standards and practices not only makes good sense in terms of a BC effort, it also makes sense from a legal standpoint as it shows that your organization follows commonly accepted best practices.

The following are some cross-industry examples of "quasi-regulations":

- NFPA 1600 (National Fire Protection Association standard).

- FEMA 141 (Disaster Recovery Planning for Business and Industry)

- DRII Professional Practices (DR/BC Best Practices)

- Basel Accord (International Finance and Banking)

- ISO 15489 (Records Management Practice)

- NFPA 232 (Physical Protection and Storage of Documents)

Note that for global and multi-national companies, the list of regulatory requirements, best practices, and standards can grow quite large. It is possible that an organization in the U.S. would also need to at least be cognizant of, and possibly comply with, foreign regulations. This could be due to ownership, requirements by customers for their vendors, or other reasons. No matter what the reasons, these requirements need to be included as part of the scope of the BCP whenever possible.

Other Keys

The following bullets represent just a few of the areas that need to be reviewed and addressed as part of a BCP effort. This provides a good illustration of the "continuation" aspect of BCP – each item below concerns an aspect of the business that needs to be addressed to ensure that the business is able to continue:

- Emergency Response (procedures, reporting, tracking)

- Executive Communication Plan (officers, stakeholders, etc.)

- Public Relations (who will represent your company to the media?)

- Damage Assessment / Insurance Claim Processing

- Employee Tracking and Communication (multiple means of two-way communication preferred)

- Ongoing communication with Customers and Vendors (you don't want to lose touch with either)

- Banking

- Human Resources and other systems that may not be deemed critical to initial business recovery efforts, but are very important in a real recovery scenario where it could be weeks or months before everything is back to normal.

- Other interfaces to customers and vendors (phone, mail, email, website, etc.)

These are the subtler and often forgotten aspects of running a business in a crisis situation that can sometimes be overlooked in a planning effort. For example, where will the mail be sent if your main building is gone or inaccessible?

A Project Methodology for BCP

For nearly all organizations, a BCP effort is a large project and should be managed as such. The Project Manager (PM) is responsible for the coordination of the efforts of the various Business Units, the IT Department, and executive management in order to achieve the final goal of a working Business Continuity Plan. The use of sound PM methodologies, such as those published by the Project Management Institute (PMI) in the Project Management Body of Knowledge (PMBOK), are essential to this process.

In an ideal environment, oversight and direction are provided to the PM by a steering committee composed of the various Business and IT leaders that are appointed by the Executive Sponsor/Champion. The PM is responsible for the overall management of the BCP effort, which may require the creation and management of smaller "sub-projects" to aid in the overall effort.

However, since conditions are seldom ideal, it is important to seek advice from both internal and external subject matter experts and business experts. This can range from reviewing the overall direction and plan with the executive board, through a review from an organization's internal Project Management Office (PMO) up to and including third-party "Independent Verification and Validation" of assumptions, direction, and overall plan.

A Phased Approach to BCP

As is the case with many projects, it is important to detect and remediate any problems that are encountered with a BCP effort as early as possible. This reduces the amount of rework required in the event problems are detected. The phased approach described below provides a logical "milestone/decision point" between the two phases of the project. This pause in execution is used by the PM to review progress with the steering committee and senior management, and is key to the estimation of the time and level of effort required by the second phase of the BCP project.

The assumption below is that the organization in question either has a working DR plan or is undertaking the creation of a DR plan in conjunction with the BC effort.

Phase I

The first phase of the BCP effort is concerned with identification, documentation, risk assessment, and impact analysis. At the end of this phase, the following documents will be created:

- Scope Statement for Business Continuity Planning (BCP) Effort

- Business Impact Analysis (BIA) Document

- Risk Assessment (RA) Document

- Single Points of Failure (SPOF) Document

Key Tasks

Task ID	1
Task	Definition of Goals, Requirements, and Constraints.
Deliverables	Scope statement for BCP Effort.
Notes	This document created by this process is the driver for the overall effort, setting forth the overall goal of the effort, as well as identifying any additional requirements and constraints. This document will identify the key stakeholders in the process, including the executive sponsor, steering committee, and any other key subject matter experts.

Task ID	2
Task	Environment Documentation
Deliverables	Business Impact Analysis (BIA) Document Risk Assessment (RA) Document Single Points of Failure (SPOF) Document
Notes	The documentation created by this task is the key driver for the determination of the BCP strategy and the creation of the BC plan in Phase II. In this task, risks are identified, prioritized, and managed; the various single points of failure for the business (including external dependencies) are identified; and the overall business impact of these risks and SPOF are calculated. This phase also is used to review any existing BC and DR documentation the organization has already created, as well as identification of any regulatory requirement and best practices/standards that need to be followed.

Task ID	3
Task	Estimates for Phase II
Deliverables	Estimate as to time and effort required to complete Phase II.
Notes	In this task, the PM works with the steering committee and executive management team to determine the level of effort and time required to complete Phase II.

Milestone/Decision Point

This built-in pause provides the ability for the BC team to evaluate the recommendations relative to their goals and budget, determine the best / most appropriate way to proceed, and create preliminary schedules and budgets based on that preliminary plan. This may mean bringing additional resources in to work on Phase II, the subcontracting of Phase II to an external organization, or even the postponement of work on the BCP until such time as the organization is better positioned (in terms of time, resources, and money) to pursue the completion of the BCP. This point also provides a logical place to bring in a third party for an Independent Verification and Validation of the work to-date, and the proposed scope and effort of the next phase of work.

Phase II

The second phase of the BCP effort is concerned with the determination of the strategy for the BC process. At the end of this phase, the following documents will be created:

- Business Continuity Plan

- Communications and Coordination Plan

- Emergency Response Plan

- Test Plan and Success Metrics for BC Plan

- BCP/DRP Coordination Plan(s) (if required)

Task ID	4
Task	Determine BCP Strategy
Deliverables	None
Notes	This uses the outputs from Phase I in order to determine what BC strategy the company will pursue. This includes determining what business functions are "core" or "mission-critical" and determining how to manage the risks identified in the risk analysis process (address, mitigate, or accept). The output from this task feeds directly into the creation of the BCP.

Task ID	5
Task	Create BCP Plan
Deliverables	Completed Business Continuity Plan
Notes	This is the main deliverable of the entire project, but it should be noted that like all of the documentation deliverables in this project this document is a "living" document and will need to be updated at least quarterly. As part of this task, any subplans (such as department level DR plans, external supplier response plans, etc) will be integrated into the completed BC plan.

Task ID	6
Task	Create Communications/Coordination Plan
Deliverables	Completed Communications and Coordination Plan
Notes	Communications is key in any crisis - the Communications and Coordination Plan (CCP) defines the types of communications that will be used during the execution of a BCP. This deliverable will document the communication channels for the organization; defines a chain of command for coordination of the BC effort; defines authorized media contacts; and includes notification procedures for key suppliers, vendors, and clients.

Task ID	7
Task	Create Emergency Response Plan
Deliverables	Completed Emergency Response Plan
Notes	The Emergency Response Plan (ERP) defines responses to emergency situations, which are defined as risks that pose a danger to life, property, or the environment. Organizations engaged in heavily regulated industries, such as manufacturing or processing, will have more detailed requirements for this deliverable than will an organization engaged in light manufacturing or sales.

Task ID	8
Task	Determine Test Methodology
Deliverables	Success metrics spreadsheet. Test methodology. Test plans.
Notes	This task defines the methodology used to test the BCP. Key questions answered here are "how often do we test?", "how much do we test?", "how do we run the test?", and "how do we judge the success or failure of the test?" The test methodology chosen is largely dependent on the organizations needs, resources, and time. The type of testing can range from minor components of the plan being tested through a full test of the entire plan (not recommended); time frames for tests can range from quarterly to yearly; and notification can range from planned to completely unannounced (i.e., surprise test). Test plans should be created with clear objectives, with each objective being defined assigned a factor denoting its importance to the overall BC effort (low, medium, high). These objectives are used to "score" the BC test, providing feedback for individual tests as well as providing ongoing metrics to compare against historical efforts.

Task ID	9
Task	Test Business Continuity Plan
Deliverables	Completed test plans Completed Success Metrics Spreadsheet
Notes	This task is an iterative task that will be performed in accordance with the test methodology defined in task #8.

Task ID	10
Task	Review, Refine, and Maintain Plans
Deliverables	Updates to all plans produced as part of the BC effort.
Notes	As mentioned above, all documents created as part of the BC effort should be considered "living" documents and as such should be updated on a schedule defined by the organization, but at the very least yearly. Of particular importance is the integration of the BCP with other plans created within the organization or by key third party organizations.

Summary

The ultimate goal of a Business Continuity Plan is to ensure the business can survive and continue to do business. Minimizing the interruption of service and loss of data will save you money and will minimize disruption to your customers and/or suppliers. Without such planning few organizations will be able to remain competitive in today's marketplace in the event of real disaster, however many organizations lack a valid, working BCP.

This whitepaper has provided a high-level overview of Business Continuity Planning, as well as defining a high level framework that can be used to create an organizational BCP. This framework includes components - such as the Business Impact Analysis (BIA), and Risk Assessment (RA) that can provide value beyond that of the BCP by exposing potential problem areas or opportunities within the organization.

For more information on Disaster Recovery Planning, please see our related whitepapers at http://www.comp-soln.com/whitepapers. Remember, if you can't continue to service your customers the chances are that someone else can and will.

About the Authors

Chip Nickolett, MBA, PMP wrote the original version of this document (which has been updated over the years as technology and practices have evolved), and has also written the majority of our Disaster Recovery white papers. He has been involved with Disaster Recovery efforts since 1994, and created the Disaster Recovery / Business Continuity Practice at Comprehensive Solutions.

Jason Schmidt has been the recovery coordinator for several high-visibility, mission critical DR projects. He assisted with the development of the BC/DR practice at Comprehensive Solutions, and contributed to the development of this document.

Let Us Help You Succeed!

Call today to discuss ways that Comprehensive Solutions can help your organization save money and achieve better results with your IT projects. We provide the *confidence* that you want and deliver the *results* that you need.

View our "Disaster Recovery" Brochure

Back to White Papers

Back to Services

Comprehensive Solutions
4040 N. Calhoun Road
Suite 105
Brookfield, WI 53005
U.S.A.

Phone: (262) 544-9954
Fax: (262) 544-1236