

12 Attributes of a Successful Business Continuity Plan

Michael J. Corby, CCP, PMP, CISSP

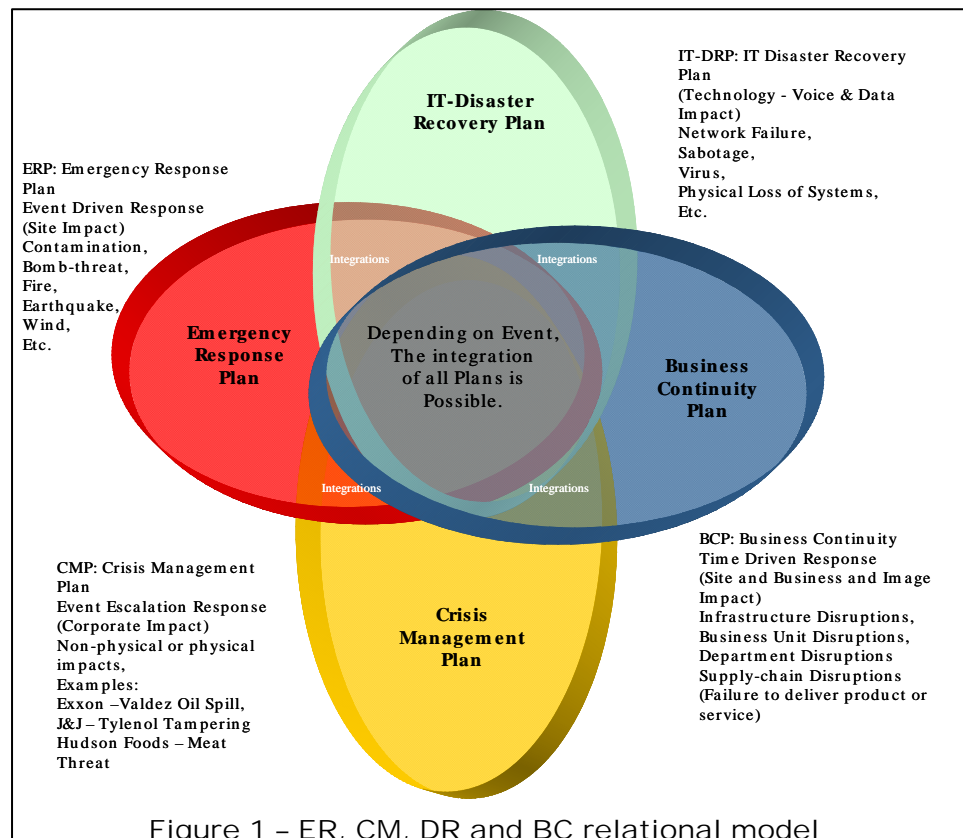
Question: What does a Business Continuity Plan have in common with a parachute?

Answer: When you find out that either doesn't work, it may be too late.

Business Continuity Planning is the one of the four commonly linked components of an organization's risk management strategy. The distinction and relationship among the four components are commonly misunderstood. Often one component is confused with the other three. Frequently all four are combined into an overall process, which is good, but then handed off to a single person, or a small team of people who are charged with trying to satisfy the basic requirements of all of them in one fell swoop. This has generally proven to be an impossible task. All are important and each one has a specific critical role to play in resolving serious disruptions, but each one is a complex process and can require the more effort than a single person or small group of people can accomplish. In Business Continuity Planning, shortcomings are like mistakes made in parachute packing. Neither one is recognized until it's too late, with very poor results. This paper will take a look at Business Continuity Planning from a unique perspective; the end.

Over many years of Business Continuity Plan development, I've come to recognize twelve telltale signs that often foretell the fate of the business continuity planning effort. Let's look at the role of Business Continuity Planning within risk management and these twelve indicators of success.

Business Continuity Planning joins with Emergency Response, Crisis Management and Disaster Recovery



Planning [see Figure 1] to create a comprehensive process for recovering from unexpected events that threaten stability or even future existence of an organization. Business Continuity is often the most crucial element is determining whether an organization can survive a major disruption over the long run. While the other three are certainly important factors in reducing damage, saving lives and re-establishing a reliable snapshot of the organization's technology infrastructure, databases and transactions, all are rendered ineffective without a sound Business Continuity Plan (BCP).

So how do we know if the BCP is functional? Well, after being very thoughtfully prepared, providing the appropriate documentation and following up with periodic tests and exercises of the plan in a controlled environment, I've seen twelve attributes that tilt the scale toward a successful restoration of business operations as quickly and as effectively as possible. These attributes do not necessarily mean the plan will be a success, nor do they indicate that failing to demonstrate them foretells failure. There are always humans going an extra step beyond their expectations, good (or bad) luck, timing and a whole host of factors that cannot be measured. But good business continuity planning is all about eliminating or reducing the dependency on these random coincidences. Without further introduction, here are the twelve attributes:

1. Critical Business Functions Have Been Identified and Prioritized

The root of a sound business continuity plan lies in the ability to quickly and accurately determine the most important business functions. To be effective, the inventory of all critical business functions (both manual and automated) must be created in advance and be accurate. This inventory needs to include factors that can change an item's priority, such as a cash management application that is extra important just before scheduled large payments are processed, like payroll, or acquired inventory payments.

Determining the truly critical applications can be a challenge. I've seen an exhaustive list of applications that have been deemed by their owners as "critical" in which everything is a #1 priority (most often this is the result of department heads jockeying for position and the designation of "most important") or nothing is important at all (often this occurs when identifying critical applications would result in substantial work to develop the BCP, so to save time and effort, nothing is critical.)

Either of these incorrect extremes can be explained, but can cripple the development of a Business Continuity Plan if it isn't corrected early on in the process. Each application must be evaluated for business impact if it were delayed or if it failed, and an appropriate priority assigned. I tell people to think in terms of a deck of 52 cards. Each card represents a business function. At arranged times of the day, or the month or in the production cycle, try to decide how to stack the cards. Which is on top? Which one is on the bottom? Which is more or less critical than any of the other ones?

Although not an exact science, typical business functions can be tied to one or more roles they play in defining a predictable operational process, and subsequently, the effect they can have on the business' success when these functions are lost or operating below par. This may be a direct financial loss, such as failure to ship a finished product, or inability to create a bill for services rendered. A function can also be evaluated for its contribution to business success in terms of

- Brand damage,
- Lost market share,
- Product failure or
- Legal/regulatory consequences.

A thorough application inventory will include which of these functions would be impacted if the business operation cannot be performed, is slow, late or incorrect?

2. **Recovery Time Objectives Have Been Determined for Critical Assets**

The impact of a loss or delay in completing a business function typically changes over time. Usually we find that most business functions do not result in a significant brand image or product creation immediately, even though the effect on product quality, regulatory compliance or direct revenue can be immediate. A temporary work-around can often be used for some period of time before the effect is actually felt, but in almost all business functions, that temporary fix can only be continued for a short time before it becomes cumbersome at best and totally ineffective. That point in time when the process must be restored is called the Recovery Time Objective (“RTO”). When connected to the revenue streams the RTO represents the maximum time that the facility, person, process or technology is unavailable or delayed until revenue is seriously impacted

Extending the RTO by creating alternate “workaround” processes or by offering other mitigating factors (e.g. outsourced or subcontracted services) is often a cost effective option. This alternate almost always requires work be done to identify and describe this process, and maybe to retain external services before the disruption occurs.

For each business function, the RTO should be estimated for both computer and manual processes or applications and should include the loss or reduced functionality of:

- People (employees, contractors, consumers, approvers, etc.)
- Process (formulas, recipes, manufacturing methods, function “run books”, etc.)
- Plant (buildings, capital equipment, warehouses, transportation vehicles, etc.) and
- Technology (computers, telephones, fax machines, copiers, measuring equipment, etc.)

Defining RTOs for each of these factors allow the Business Continuity Plan to be an effective tool for all types of events, including flu epidemics (people), internet connectivity issues (technology), fire (plant) and additional product suppliers (process).

3. **Recovery Point Objectives Have Been Established for Critical Applications**

Recovery Point Objectives (“RPOs”) are similar to Recovery Time Objectives except that they represent the tolerance for lost data once the process has been recovered or restored. For most computer applications that require data entry, archiving the source documents for re-entry will support full data recovery however the source documents may be lost or destroyed along with the computer files. Effective file and document archive procedures can help prevent losing these critical transaction records entirely.

Technology has advanced to the point where critical data files can be maintained and synchronized in more than one location, enabling a potential RPO of zero to be achieved.

4. **A Comprehensive Risk Assessment Has Been Conducted On Critical Facilities**

The risk of loss of critical facilities can be mitigated, but generally at very high costs. Successful Risk Management methods strive to achieve a risk mitigation strategy that is proportionate to the potential for loss. There have been numerous attempts at detailing the steps required for a thorough risk assessment strategy. As in many other processes, perfection is the enemy of the good. I’ve seen organizations get so mired in the details that the objective can never be met. If risk management efforts start at the lowest level of detail, chances are pretty good that before all the details have been tallied, the cost factors will have changed. Then what do you do? Too frequently the answer is to start all over.

Some Business Continuity Planning projects start by listing every possible scenario, from rainstorms to global thermo-nuclear war. By the time all these scenarios are listed, and all the possible effects on every item and building in the organization, what you end up with is very close to an infinite-by-

infinite matrix to solve for the most likely events. Its much easier to look at the four key elements of People, Process, Plan and Technology and to ignore the event that can cause a disruption, but instead look at the effect on those elements in only two categories: Total Loss and Significant Reduction in functionality. That transforms the target of the risk assessment from an infinite by infinite matrix by a much simpler four by two matrix. Only eight possibilities for each critical business function. By my calculation this is a much more attainable result.

In an overall enterprise strategy, the most common mitigation technique is to identify and prepare alternate sites for all critical elements. In other words, no single point of failure. The old US space program had it right: redundancy upon redundancy, or as lampooned by the often quoted 60's comedy troupe: *Firesign Theater*: become the "Department of Redundancy Department".

Finally risk assessment isn't a document; it's a process. In selecting alternate facilities or sites, failover plans should be tested regularly and temporary assignment of key staff members should be included in the test plan. A professional athlete doesn't stop practicing when the contract is signed (with some notable exceptions). Improvement can be best attained through repetition and practice.

5. Succession Plans Exist for Key Employees or Consultants

One of the most overlooked aspects of successful Business Continuity Planning is the potential loss of key decision makers during the response and recovery time when their abilities are most crucial. If you want to see the impact of key decision makers in a Business Continuity Plan, try running a recovery test without certain key roles. Often the head of Corporate Communications, the Data Center Manager, the I/T Network specialist or the authentication server administrator has knowledge that eluded the recovery documents. The obvious scenario is that these people were casualties of the event, but to offset a morbid test environment, try declaring that these or other key positions are "on their honeymoon" or "sick with the flu" or "having a baby". Then put the alternate in charge of that function and invite the "missing" incumbent to observe the decision making, but forbid them from participating or providing direction.

As a checkpoint in the Business Continuity Plan, select an alternate for each critical staff position, who is asked periodically to perform response and recovery functions in place of the incumbent during planned tests. This should become a documented element in all job descriptions and performance review standards.

Interestingly, a good succession planning policy has an added benefit in that it gives employees a clearer way to manage their career advancement, resulting in more favorable employee turnover and improved productivity. With the cost of replacing and retraining good employees, this simple process can be turned into money in the bank!

6. A Technology Backup Strategy Exists and Is Tested Regularly

Several years ago, an interesting I/T disaster Recovery approach developed. Called the "No-Plan Plan, it prescribed that every day should be a Disaster Recovery exercise. Back in the 1970's I worked at a company that ran its nightly applications in this way. All data files and programs were stored on tape (primarily to offset the high cost of disk storage at that time), and every critical computer system started with a step that restored the programs and data from the tape to the disk, followed by execution of the application, and concluded with the creation of a new tape for use in the next scheduled processing. Coincidentally, it was an excellent technology recovery plan in that it could be easily transported to any of a couple dozen nearby data centers that had compatible computers, and run completely with minimal disruption of the new host.

Too often however, I/T Disaster Recovery Planning is confused with full Business Continuity Planning, but in reality it only represents part of the enterprises risk management strategy. I/T recovery can be fruitless if there are no available people or facilities to use the restored computer applications. Creating and testing is an effective element in Business Continuity, but it cannot become the sole activity.

The good news is that although since 2001 many companies have downgraded the services of commercial data center “Hot Sites” to a lesser role during actual recovery, they do continue to represent a basis for I/T Recovery testing, and are frequently exercised. Even when self-contained recovery strategies replace commercial resources on an evolutionary basis, these changes become a part of the more comprehensive recovery program.

Finally, it’s not unusual to spend considerably more time planning a Disaster Recovery test that doesn’t create an interruption than running the test itself. Data privacy and security must always be maintained, even during recovery. One philosophy I’ve used over the years is “Don’t create a disaster trying to test the recovery from one”.

7. Multiple Sources Are Available for Critical Supplies and Processes

Product quality and information privacy regulations make the task of identifying alternate suppliers more challenging. You cannot relinquish your need for proper controls over your alternate sources.

Purchasing Departments have traditionally been able to identify sources of materials, but will always need additional support in finding alternate suppliers of technical processes and business services. This is particularly true in the industries where regulatory demands impose consistency and quality expectations like food, cosmetics, toys and pharmaceuticals. Approval of alternate suppliers or alternate processors can require months by the approval agencies, and production may be limited or unavailable while this approval is obtained.

Remember also that shortages of common resources can affect many companies in the same industry. Recent efforts have been fruitful in building supply-chain resources in collaboration with other organizations, even competitors. If your company is one of several that makes widgets using gizmos, the entire industry segment is affected when there is a gizmo shortage.

8. People, an often overlooked critical business resource, are included in Business Continuity

Recently, pandemic response planning has taken its place in Business Continuity Planning, both from an employee absence perspective and one that represents a dramatic alteration in public behavior. (e.g. restaurants, public transportation, hospital care)

Many situations less severe than a widespread disease pandemic can be effectively built into Business Continuity Plans. Effective plans include alternates for key contributors, and a process for enabling a productive and secure Small Office/Home Office (“SOHO”) environment. In one instance, a company whose offices were located in an urban skyscraper were informed that another tenant in the building had an employee who unknowingly came to the office with a contagious case of the measles. All tenants were notified that they could expose pregnant employees or family members of employees who rode in the same elevator bank to this disease. As a result, alternate plans were drawn up so that employees concerned about this exposure could continue to work without physically coming to the office. Pandemic? Not really, but a very real health situation.

Recent experiences with regional disasters such as floods and hurricanes have also resulted in more refined plans to assure that family members and household stability can be assured before employees can be productive.

9. Tools and Training Are In Place to Provide Advanced Warning of Incidents

The best Business Continuity Plans are ones that can be initiated very early before the interruption has progressed to the point of a crisis. Well trained and practiced employees are the first line of defense in identifying situations that could become serious. Part of the plan is to teach employees to recognize the signs of an impending disruption in normal activity.

Many computer incidents such as failing components, hacking attempts or infection by computer viruses or can be recognized by intrusion detection and operations management tools. These components are often included in technology operations strategies, **but** they must be run and monitored to be effective.

To aid in identifying these impending disruptions in technology, I/T help desk incident correlation programs or services have become key components in identifying even very subtle signs of an imminent disruption. There may be similar advance warnings for critical supplies, short term financing, and business partner relations.

10. All Projects Include a Disaster Recovery Component

For complex I/T applications, experience has shown that developing disaster recovery elements after the application has been completed costs much more than anticipating DR needs during the design stage. Operational sync-points and offline versions of key data files can more easily be accommodated at the onset of the project.

Many effective techniques exist for building a resilient facility that can provide risk remediation, especially for computer and communications capabilities. This capacity is often cost prohibitive in existing facilities, but over time, as plants are expanded, upgraded or acquired, these modifications can be made with minimal increased cost.

The most effective Business Continuity plans have sound alternative procedures and process recovery instructions included in the project documentation. Training then includes not just regular operation, but alternatives when critical resources are unavailable.

11. Technology Domains Are Defined to Include Business Continuity and Security

Technology can be used to effectively create a domain structure that enhances the ability to consolidate resources with similar requirements for Confidentiality, Integrity and Availability. Technical infrastructure and advanced processes can be applied at the domain group level, saving considerable costs and substantially reducing complexity.

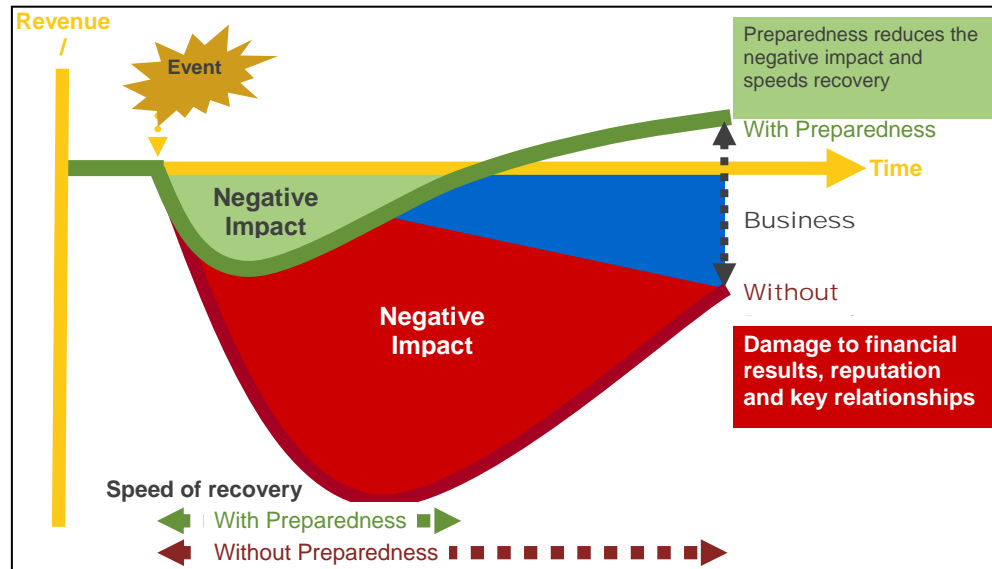
Most business units cannot justify the expense associated with providing a continuous availability strategy, rigorous monitoring or enabling strong authentication techniques. When several business units share the benefits and costs however, the expense can be more easily justified.

Damage assessment and recovery planning can frequently be streamlined if the resources most sensitive to delay or disruption can be quickly identified, salvaged and restored. Potential lost revenue is generally reduced when critical business operations are restored more quickly.

12. Capacity Planning Includes Strategy for Increased Demand

Business Continuity Planning is not exclusively for the restoration of processes after a disaster or disruptive event. Successfully executing an effective plan can also provide considerable benefits including increased market share.

Like the old joke about the two guys in the jungle trying to outrun the tiger, Business Continuity Planning is the ability to respond more quickly and more successfully



than competitors to gain a competitive advantage. Of all the companies I’ve worked with over the years, pretty much all of them have been able to recover from a disruptive event. . .eventually. All of them also could have recovered more quickly and more easily if they had done something just a bit differently. As shown in the graphic, being prepared gives you the advantage of getting “back in business” sooner than your competitors.

Many factors can have a dramatic effect on sales or transaction volume. A process or technology that is unable to meet dramatic unexpected demand can result in an ultimate loss of customer satisfaction and actually reduce your market share, even in a rapidly expanding market sector. For example, transportation costs, technology changes or imminent weather conditions can cause a dramatic increase in demand. Thorough Business Continuity Plans often include these dramatic increases in demand as well as loss of functions.

One way to do this is to develop a strategy that establishes external services to provide an expandable production capacity. If these suppliers are used for a portion of the normal production, the process is already in place. Connections, order management and quality assurance functions can be counted on to provide an effective mitigation technique that can expand facilities or capabilities whose demand has exceeded their capacity.

So there you have it: twelve telltale signs that you may be on the right track. All of them can be worked at, improved and deployed throughout your organization. Are you ready? Hopefully you are. If not, do you feel lucky?