Robyn Loftin

GSEC Practical Assignment
Option 1
April 7th, 2004
Version 1.4b

Preparing for the Worst: The Preparation, The Execution, and The Evaluation of Business Continuity Exercises

Table of Contents

Testing a Business Continuity Plan

Abstract:

With the increasing height of terrorism and the threat of natural disasters always looming, a Business Continuity Plan can be the determining factor as to whether or not a company survives a catastrophe. With this in mind, it is ever important to frequently test continuity plans to assure every aspect required to continue the business is considered. A business' every day process is not secure without a thoroughly tested continuity plan.

This paper will discuss the how and why of exercising a continuity plan and will walk through the process. Before explaining the different continuity exercises, this paper introduces continuity planning, why testing is crucial to its success, and continuity testing methodology. There are many decisions to be made when planning to exercise a business continuity plan but the most important one is the decision to test the plan itself. This paper will begin with what a business should know before testing their plan. Then it will address the differences in continuity exercises. Finally, this paper will explain ways to evaluate and combat known vulnerabilities after testing. The reiteration of the importance of testing and a summary of the exercise process concludes this paper.

An Introduction to Continuity Planning:

Before a Continuity plan can be tested, one must understand its purpose, the importance of testing, and test methodology.

A Business Continuity Plan is a structured document containing the actions to be taken in the event of a disaster. These actions should be documented in such a manner that the people and systems affected are able to resume normal business functions in the shortest amount of time possible after the disaster.

Continuity plans can approach the recovery process with different strategies. MasterCard International employs one example of continuity strategy. This strategy begins with risk assessment, continues into disaster response and communication, recovering operations as the next step, which leads to restoring regular business functions, and completes the process with continuing continuity training (MasterCard International).

Whatever strategy the business chooses, the ability for employees to continue performing their job responsibilities with little interruption of business is the essential goal of a continuity plan. Thorough contingency planning can help to assure a company is prepared to react to any outages or disasters in order to achieve their continuity objectives.

In today's world there are many examples of why continuity planning is imperative to the security of an organization. After the attacks on September 11th 2001, companies are beginning to realize that just as evacuation plans can mean the difference between life and death for their employees, having a reliable business continuity plan in place can mean the difference between life and death of the company (Wieczorek xiii).

Why is the testing of a Continuity Plan critical?

The only way to ensure the continuity plan will meet the company's expectations during a disaster is to rigorously test the plan. A strict business policy enforcing regular and thorough testing exercises is critical to a recovery plan. Malcom Cornish, managing director of Recovery Management International, had this to say in regards to the importance of testing a Continuity Plan "I would argue that having a plan and not testing it is more risky than not having a plan at all and creates complacency and a false sense of security amongst senior executives" (Cornish).

A company's chance of surviving disaster dramatically increases when a regularly tested continuity plan is in place (UK Resilience). The purpose of testing the plan is to identify weaknesses and then update procedures in the plan to account for those identified vulnerabilities (UK Resilience). Exercise participants who would be involved in the recovery process are provided the chance to practice their recovery role in a controlled environment as opposed to performing their recovery duties for the first time during an actual disaster.

Plans are tested to prepare for any kind of disaster that puts the continuity of business operations at risk. Disasters can be broken down into the following three main categories:

“Natural	Environmental	Incited
Flood	Aircraft crash	Arson
Hurricane	Explosion	Sabotage
Earthquake	Contamination	Vandalism
Tornado	Communications	
Fire	Power” (Myers 27).	

A continuity plan should not be considered ready for an actual disaster situation until it has been thoroughly tested and proven to be a viable recovery resource for the company. Knowing the business’ continuity plan and exercising that plan can help reduce “decisions, confusion, recovery time, and the cost of recovery“ (DRI 2.6).

All areas of a business should recognize and respect the importance of understanding their continuity plan and the recovery process. In order for continuity testing to be a success, the individuals organizing and participating in the recovery exercises must approach this in a professional manner and be committed to the process (BCI). All levels of an organization should be involved in and support continuity testing including employees, management, directors and executives (BCI).

The Methodology of Continuity Testing:

There are many ways to exercise a continuity plan but the theory behind the complete process or methodology of testing can be broken down into the following five phases as explained in the Disaster|Line website:

I. “Plan Audit”
II. “Plan Walk –Through”
III. “Scenario Workshop”
IV. “Physical Test”
V. “Live Simulation Test” (BELFOR-Relectronic)

While not all businesses will choose to complete all five phases, it is important for a company to understand the benefits of each phase. Examples of how each phase is executed will be discussed in the next section.

The first phase of this methodology referred to as “Plan Audit” will determine whether or not your continuity plan is ready to be tested. At this point, the plan should be reviewed for out of date content and ensure any other updates have been included to assure all information is correct for testing. Not only should the plan be up to date with current information but the plan should also be reviewed to judge its effectiveness (BELFOR-Relectronic). If weaknesses are identified in the plan during this phase, suggested updates should be made before moving on to the next phase of testing (BELFOR-Relectronic).

After the plan has been reviewed and the okay has been given to proceed with testing, the “Plan Walk – Through” is the next step. During this phase, everyone who plays a role in the continuity plan should be involved. It is important that all people crucial to the process be included in the walk-through in order to become comfortable with their role in the plan. All members of the recovery team should be secure in their role and understand the logical flow of the plan before moving on. Under prepared team members may hinder the recovery process.

When everyone is familiar with the plan, “Scenario Workshops” should begin. Management will lead a recovery team through a disaster scenario during which participants are expected to work through the simulated disaster in order to recover business operations (Wieczorek 120). If all goes well during this exercise the employees will each know their role and work together to ensure the continuity of their business will not be at risk in an actual disaster.

With the success of the “Scenario Workshops” we move into the fourth phase of testing which becomes even more realistic, the “Physical Test.” The simulated recovery process now takes place at “a readied location to be used in the event of a continuity threat” or a recovery site (Business Continuity Planning Asia). How participants react to the situation and their confidence in solving problems should be noted during this process (Wieczorek 118-122). The data derived from this exercise will be evaluated at the end of testing. The different means of evaluating test data will be discussed later on in this paper.

A “Live Simulation Test” is the final and most thorough phase of testing methodology. This phase can include personnel outside the recovery team who would also be involved during an actual emergency (Sebastian). Due to the size and effort of this phase, “Live Simulation Tests” should only occur after the four prior phases are successful (BELFOR-Relectronic). Simulated disasters could include tornados, large hail, fires, or even terrorist attacks. The simulated disaster does not always have to be of large proportion to pose a continuity threat. A small fire in a room containing many servers could pose a large business continuity threat. The continuity plan should be flexible in order to recover business operations after any type of disaster.

Preparation:

After understanding what a continuity plan is, why it should be tested, and exercise methodology, the exercise process may begin with the preparation phase of plan testing. Preparation should include meeting with management, identifying exercise participants, ensuring an adequate location for the exercise, and monitoring the process which includes establishing how test results will be evaluated.

Management should be involved from the very beginning of this process. The team responsible for testing the plan should meet with management as the first step of preparing for continuity testing (BCI). This meeting allows management the opportunity to voice any concerns and/or their expectations during the testing process. The result of this meeting is for management and the testers to draw up a testing agreement (BCI). This process includes determining the scenario to test through, assessing the risk of the exercise, assuring production is not hindered by the test, and preparation of documentation to be used (BCI). The testing agreement would include the exercise information agreed upon by management and the recovery team. Working with the management of the work area to be exercised is one of the first crucial steps in the process of a successful continuity exercise (UK Resilience) “Successful organizations have discovered that management sign-off on the test plan leads to increased business unit support and attention to detail” (Zawada).

The identification of exercise participants should be one of the first pre-planning objectives. Involving all the necessary individuals who will play a role in the recovery process is imperative to the continuity exercise (Zawada). Not only should primary recovery team members be involved, but also any alternates who would be responsible for a part of the recovery process should the primary person be unavailable at the time of a disaster (Zawada). Involving all participants in the exercise is crucial because “the people that implement the plan and the recovery or resumption activities in general are arguably more important than the plan itself” (Redmond 1). A plan is only as prepared for execution as the people are to execute it therefore it is not only the plan that is being tested but also the knowledge of the participants.

If the exercise is one that requires an alternate location, the technical capabilities of that alternate site should be examined thoroughly to ensure the area can support the technology being brought in as part of the exercise (Redmond 1). Technology is a large part of business today and it plays a large part in the recovery process. If the site is not adequate or prepared for testing, participants may become unhappy with the recovery process which would in turn prevent the recovery team from attaining their goal to successfully execute the testing process (Redmond 1). Reviewing the plan for technological requirements and assuring those capabilities will be available at the recovery site for the exercises is critical to the process.

The last consideration in the process of exercise preparation is how to monitor the exercise and coordinate the process from start to finish. Items that fall into this category can vary. The simple decision of when to begin and end an exercise is an example of a piece of the monitoring process (Zawada). Assuring all areas that will be participating in the exercise are communicating with other affected work areas is another example (Zawada). Each area must be aware of the recovery steps other business areas are taking in order to coordinate and promote the recovery process. The monitoring process also includes the handling of exercise data and evaluation techniques. Evaluation techniques and criteria should be established during this preparation period (Zawada). The predetermined evaluation techniques are critical to the testing process because that data will provide the business with the information required to strengthen the continuity plan.

Exercising the Plan:

When the preparation process has been completed, then testing should begin. The exercise chosen during preparation is specific to the need of each business. Some businesses with higher risk will choose more rigorous and extensive tests, but others may choose a simple walk-through exercise. A continuity exercise can be defined as the following "An important management tool for informing and motivating personnel and giving confidence to those who may be required to respond in a crisis" (UK Resilience). The following are the varying degrees of continuity tests:

• Awareness	- introductory training
• Desktop	- verbal scenario walk-through
• Scenario	- actual acting out of role
• Technical	- testing technical limitations
• User	- executed on actual test site

(Wieczorek 118-122)

Again, not all companies will choose to complete each type of exercise, but it is important for business' to understand each in order to asses their needs.

"Awareness" training is the most basic way to exercise your continuity plan. The goal of these sessions is to simply inform employees of their business continuity plan. At then end of this training, participants should have an understanding of the need for continuity planning and be familiar with their business' plan for continuity (Wieczorek 118-122).

One approach to "Awareness" training can be accomplished with two training sessions. "Introductory awareness training" is for participants indirectly playing a role during the implementation of the continuity plan and "Detailed awareness training" is for participants who play a primary role in the recovery process

(Morwood). Introductory training should deal with different emergency processes and procedures and could be accomplished in approximately one hour (Morwood). Information provided during detailed awareness training is more in depth therefore training may last closer to a half a day (Morwood). The material covered there should resemble the information covered in the introductory class but it should also provide more details about specific recovery roles and how they might be affected by other business areas (Morwood). During "Awareness" training, it's not the companies' specific plan that is being exercised, but the business recovery knowledge of its employees. This type of exercise may be the only type of continuity training for a smaller company, but also may be the beginning of continuity testing leading up to a simulated exercise for larger companies.

Although awareness training may seem simple, it is a very important step in becoming more secure with a continuity plan. Whether an employee's role be direct or indirect, it is important for employees to attend awareness training in order to be prepared for the recovery process in the event of a disaster (Morwood).

The next type of test is referred to as a "desktop" or "tabletop" exercise. A "Tabletop" exercise is conducted in a regular business environment by a facilitator who creates a scenario ahead of time and then provides the situation to the recovery team at the time of the exercise. The process of this exercise can be administered in four steps including Introduction, Scenario Presentation, Simulation Exercise, and closing (Hayes).

The introduction process for a "tabletop" exercise is fairly simple. The facilitator identifies each person in attendance to ensure the correct people are present, assures everyone is familiar with the continuity plan about to be tested, and checks to see participants are comfortable with their role in the process (Hayes).

Once the introduction is complete, the facilitator will provide the recovery team with specific information regarding the disaster situation. After the scenario has been explained, the facilitator should ask for any questions and both the recovery team and the facilitator will determine any "assumptions" (Hayes). An example of an "assumption" would be establishing that network connectivity was unavailable.

The facilitator should then begin the exercise with questions directed at the recovery team regarding their recovery process. Examples of facilitator questions are "Who does what first and/or next?" and "What is the timing or sequence of this action?" (Hayes). It is the recovery team's responsibility to answer these questions while utilizing their continuity plan. The facilitator should continue to change the situation based upon the recovery team's answers in order to identify plan vulnerabilities (Hayes). Problem areas identified during this process should be tabled for discussion before continuing with the exercise.

In the closing of the exercise, the facilitator should assure all problems or questions have been addressed and assign someone to be responsible for updating the continuity plan with procedures to combat discovered plan weaknesses (Hayes). Without the required updates, the problem areas identified during testing will remain a threat to business continuity.

The goal of a "tabletop" exercise is to ensure the recovery team is familiar with the flow of the recovery process. This exercise can be challenging because the scenario changes and the recovery team must know where to look in their plan to propose the next logical step in the process (Wieczorek 118-122). The benefits to this exercise are familiarizing participants with their role in the recovery process and introducing them to other recovery considerations. These considerations could include the possibility of loss of power or other resources that may not have been discussed prior to testing.

A "desktop" exercise is more involved than awareness training but not as involved as "Scenario testing." In a Scenario test participants will act out their role in the recovery process (Wieczorek 118-122). It is most often that these participants are directly related to business recovery (Morwood). Scenario testing can be completed in four phases: planning, warning, execution and validation (Morwood).

The planning phase may include many routine checks completed prior to any scheduled continuity testing. These checks establish goals and the means for determining the success of the test. The specifications of the test itself should be decided upon by management and the recovery team. It should then be ensured that management, and any other areas being affected, support the exercise before continuing with the process (Morwood).

This approval from management and other affected areas can serve as a part of the warning phase. The purpose of the warning phase is to ensure that all participants, management, and other affected areas are aware of the exercise timeframe so as not to impact the production environment (Morwood). The affect testing will have on regular business processes should always be considered before testing.

The execution phase should include the acting out of the recovery process based upon the scenario provided to the recovery team (Wieczorek 118-122). The exercise will be most beneficial to participants if all the aspects of recovery are incorporated into the plan. This allows the recovery team the chance to combat any problems in a testing environment and will allow them to feel even more secure with the process in the event of a disaster (Wieczorek 118-122). The more familiar participants are with their plan, the faster business operations can be restored.

The validation phase of “Scenario testing” is similar to last phase of other exercises. This is the review of the exercise in an attempt to identify plan weaknesses. This phase also includes the updating of the continuity plan where breakdowns in the recovery process occurred (Morwood).

The fourth type of contingency test is referred to as the “technical test.” This test has very specific technological objectives. The goal is to test the technical capabilities of the participants and to make them more confident with the process of restoring a technical work area (Wieczorek 118-122). This exercise is specific to the professionals responsible for recreating technical environments in another location as a result of a disaster.

After implementing the exercise to recreate this technical environment, the data should be reviewed to determine how to decrease the time it took to re-establish connectivity. Both the technical knowledge of the participants and the functionality of the equipment are being evaluated. If there are problems on either side which slow the process, a change in the plan should be made to compensate for human or technical error.

The last type of contingency exercise to be discussed is referred to as a “User” or “Live” exercise. This is also known as a “Dress Rehearsal.” This exercise occurs in the environment that would be utilized in the case of an actual disaster (Wieczorek 118-122). Out of all the exercises discussed previously, a live exercise should be the closest to resembling the recovery process after a catastrophe has threatened the continuity of business. Like other exercises, there are similar planning, execution and evaluation stages to this test. Employees involved directly or indirectly with the recovery process are included in a “Live” continuity test. Due to the number of employees involved, there is a large cost associated with live tests. Therefore, only some businesses will use a “Live” exercise to test their continuity plan.

The goals of the “Live” comprehensive continuity test are: implementing the continuity plan as realistically as possible, evaluating the actions taken by employees to combat the situation, reviewing the recovery process timeframe, and ensuring continuity can be restored (Wieczorek 118-122).

After the Exercise:

At the end of the exercise there is still work to be done before considering the process complete. The plan should first be validated to ensure it meets expectations by evaluating test data. Then participants and management should be informed of test results. Finally, the plan should be updated to account for identified weaknesses (Redmond 3). To validate, educate, and update are the goals of the recovery team after testing is complete (Redmond 3).

There are many ways of evaluating test data in order to validate the continuity plan. These evaluations will normally fall into two categories. The first category is “Observation or Subjective” (DRI 2.55). Results falling into the observation category are derived from what an observer witnesses during the process (DRI 2.54). The second category for evaluation is the “Documentation or Objective” category (DRI 2.55). Results classified in the documentation category are actual “measurable objectives” such as recovery timeframe (DRI 2.55). Some people respond better to results documented in numbers or statistics and other prefer first hand feedback. In the documentation or objective category the continuity exercise can be evaluated by a checklist which includes all of the original goals and a rating system to determine the success of each part of testing (Morwood).

The recovery team can validate the plan using both “quantitative” and “qualitative” information. Documented numbers and statistics are examples of quantifiable results; however, not every aspect of continuity testing can be measured by numbers. Therefore qualitative results should also be included in the evaluation (Redmond 2). One example of qualitative results is immediate feedback from exercise participants (Zawada). An evaluation including both qualitative and quantitative information should be easily understood by both management and participants.

The second part of following up after a continuity exercise, is assuring the participants have updated information about the exercise in order for them to understand plan weaknesses. Whatever exercise criteria is used, a copy of the final report should be sent to management detailing the “lessons learned” and the benefits of exercising the plan (Redmond 2). It is crucial for all to be informed because “provision of a succinct report of successes and failures to which management can refer is a vital part of the overall learning process” (UK Resilience). The sharing of this information ties in with the third step in the post exercise process – plan updates (Redmond 3). Updated plans should be available for all participants and management to view.

The following steps should assure plan updates are thorough and are completed in a timely manner:

- Delegate the responsibility of updating the plan to one person
- Set a timeframe for the completion of updates
- Check to see that changes identified by the exercise have been made

(DRI 2.59).

Developing Continuity Exercise Policy:

Before considering the continuity exercise process complete, policy should be in place not only to test the plan again, but also the designation of specific times or criteria which pose a need for a continuity test. Most plans are tested at least annually or biannually. Large changes in the business process will dictate a need for further testing. Some examples of these business changes are:

1. Change in business goals
2. Change in “strategy” or “scope”
3. Business site has changed
4. Employee numbers have drastically increased/decreased
5. Change in vendors or “suppliers”

(BCI).

Another change in business which would dictate the need for a continuity test would include technological advancements or new continuity team members (Zawada). Testing after these events occur will help to ensure you plan is up to date with changing business processes or information. In the end, it is not the determining factor which leads to scheduling an exercise but the exercise itself that is truly important. Continuity exercises should occur on a regular schedule unless one of the aforementioned changes occurs first (Zawada).

Conclusion and Summary:

It is important that everyone involved in the recovery process understand what a continuity plan is, why it should be tested, how to test it, and how to handle test results. It just takes one disaster to understand whether or not your continuity plan will successfully restore business operations, but that time should not occur during an actual disaster. Having a thoroughly tested continuity plan is a type of security every business hopes they will not need to employ. However, should the need arise to implement the plan everyone involved in the recovery process should be comfortable with their role and how the process works.

The different continuity tests available make it easier to choose an exercise that meets a business’ specific needs. A smaller company with less at risk would be more likely to choose awareness training or a tabletop exercise to test their plan. A larger company with much more at risk may select a live simulation exercise to ensure they could survive a major disaster. These varying levels of testing allow for differing degrees of testing with awareness training being the simplest and a live simulation test being the most complex.

The work done after the exercise is as important as the exercise itself. The data must be collected and evaluated whether through discussion with participants, rating sheets, or statistics. Results should be reported in a way for each participant and management to understand the strengths and weaknesses of the plan. It is then up to the continuity team to develop solutions and update the plan for participants and management to review and learn from.

An educated recovery team in conjunction with a strong business continuity plan should produce positive test results. Should these results not meet expectations, the company has the opportunity to update the plan in a controlled environment.

A well tested continuity plan with favorable results should ensure a business will survive potential disaster situations.

Works Cited

Business Continuity Asia. *Glossary of General Business Continuity Management Terms.* 4-05-2004. http://www.bcpasia.com/glossary.htm.

Business Continuity: A Must for MasterCard. MasterCard International*.* 4-05-2004 http://www.mastercardintl.com/docs/business_continuity.pdf.

Business Continuity Exercises From Disaster | *Line.* BELFOR-Relectronic (UK) LTD. 4-05-2004 http://www.disasterline.com/Buscont.htm.

Business Continuity Management – Good Practice Guide. The Business Continuity Institute (BCI). 4-05-2004 http://www.thebci.org/BCI%20GPG%20-%20Stage%205.pdf.

Cornish, Malcolm. *How Genuine Is Your BCP?.* Globalcontinuity.com. 4-05-2004 http://www.globalcontinuity.com/article/articleview/487/1/31/.

DRI International. DRP – 113 Implementing and Testing the Business Continuity Plan*.* 2002.

Hayes, John M. *Business Continuity Planning Tabletop Exercise white Paper.* Ernst & Young LLP's (E&Y) Information Systems Assurance & Advisory Services Practice. 4-05-2004 http://www.drj.com/new2dr/toolchest/tabletop.pdf.

Morwood, Gregory. *Business continuity: awareness and training programmes. KPMG Management Consulting*. 4-05-2004 http://www.managementfirst.com/strategy/curves/disaster/Business%20continuity%20awareness%20and%20training%20programmes.pdf.

Myers, Kenneth N. Total Contingency Planning for Disasters: Managing Risk…Minimizing Loss…Ensuring Business Continuity. New York: John Wiley & Sons, INC., 1993.

Redmond, Gary. Exercising Business Resumption Plans*. Business Continuity and Resumption – The Readers' Series* vol 2 (2003) 1 -3.

Sebastian, Ryan. *Business Continuity Planning and Disaster Recovery*. 4-05-2004 http://www.cccure.org/Documents/RyanSebastian/bcpanddrp.pdf.

Why Exercise Your Disaster Response. UK Resilience. 4-05-2004 http://www.ukresilience.info/contingencies/business/exercise.htm#benefits.

Wieczorek, Martin, Uwe Naujoks, and Bob Bartlett, eds. et al., IT Risk Management for international corporations: Business Continuity. New York: Springer-Verlag Berlin Heidelberg, 2002.

Zawada, Brian. *Business Continuity Plan Testing: Considerations and Best Practices*. Protiviti Inc. 4-05-2004 http://www.knowledgeleader.com/iafreewebsite.nsf/content/SecurityBusinessContinuityPlanTesting?OpenDocument.