

Overview of how to test a Business Continuity Plan

Prepared by:

Thomas Bronack

Phone: (718) 591-5553

Email: bronackt@dcag.com

Table of Contents

BCP/DRP Test Plan.....	3
Overview:.....	3
Creating a BCP Test Plan	3
Table of Contents for Technology Test Plan Template.....	3
The Contingency Organization in Action.....	4
Testing and organizational acceptance	4
Maintenance	5
Information update and testing.....	5
Testing and verification of technical solutions.....	5
Testing and verification of organization recovery procedures.....	6
Treatment of Test Failures	6
The Systems Development Life Cycle	7
Elements of the BCP/DRP Test Plan	9
Plan Audit.....	9
Passive Walk Through	9
Scenario Workshop	9
Physical Test.....	10
Live Simulation Test.....	10
Forms used to Support BCP/DRP Implementation and Test Plans	11
Level 1 - Executive Awareness and Authority	12
Level 2 - Plan development and documentation	12
Level 3 - Management & Recovery Team Assessment and Evaluation for Effectiveness	14
Level 4 - (Certification) Management & Recovery Team Assessment of Readiness and Plan Maintenance	16

BCP/DRP Test Plan

Overview:

The fundamental goal of Contingency Plan Testing is to carry out all the steps documented in the contingency plan. However, during a test this may not be probable. The Test Plan permits a plan to be tailored for testing without modifying the actual contingency plan.

The goal of this document is to identify the sections of the plan to perform, additional tasks required for testing and those tasks in the plan that cannot be completed because this is a test.

Furthermore, this Test Plan helps out in analyzing the performance of the test by rating the outcome of the activities performed during the test. Rating each task shows areas where the test team did extremely well and areas requiring attention. In addition, rating the tasks aids in ranking the overall objectives and in turn, the success of the test.

Creating a BCP Test Plan

A BCP Test Plan is created when a potential disaster event is identified and its impact calculated. Then the associated BCP/DRP document is selected, its team leaders and members identified, and the steps needed to respond to the disaster event reviewed to determine how to best benefit from the test, its desired goals and objectives, and the time frame needed to complete the BCP Test.

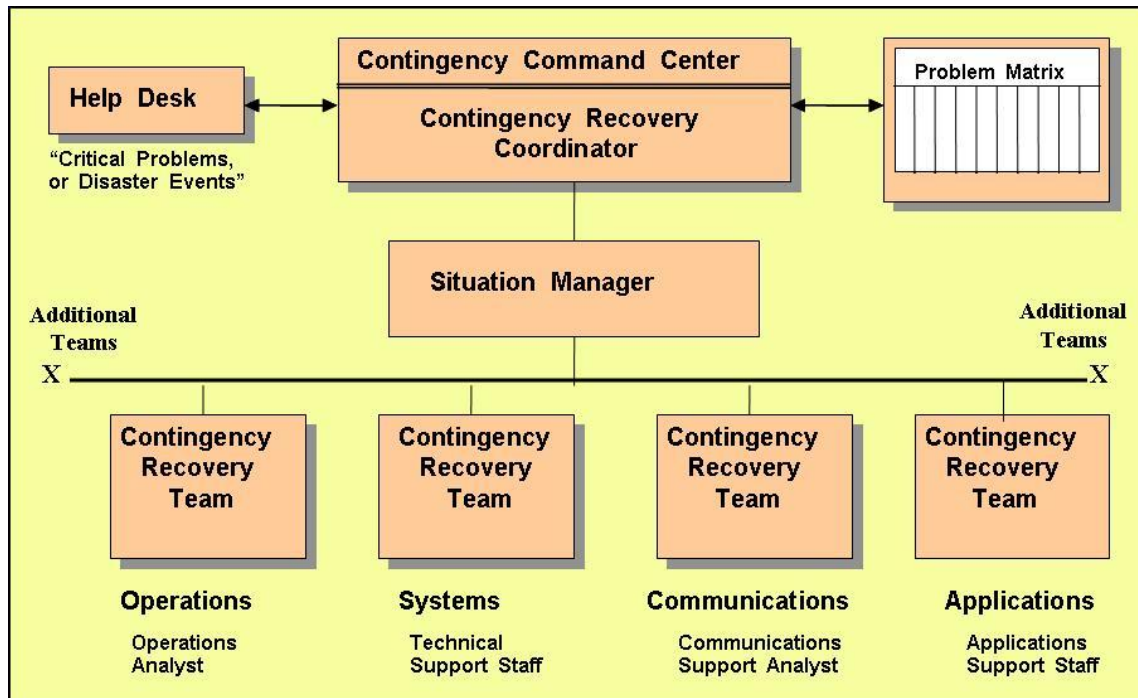
A Test Scenario is formulated and Test Scripts generated for Recovery Team members. Additional problems may be inserted to see how well team members respond to unexpected events. All actions performed during the tests should be documented and a list of problems completed for future review. Problem resolutions should be incorporated into the next maintenance phase of the BCP/DRP manual.

Table of Contents for Technology Test Plan Template

- Test Overview
- Plan Information
- Test Type & Elements
- Test Participants
- Test Scenario
- Test Scripts for Team Members
- Leverage Testing

The above is an example of what would be included in a BCP/DRP test document. All participants should be provided with the test document and any suggestions for improvement solicited.

The Contingency Organization in Action



1. When problems arise they are reported to the Help Desk. If the problem is a disaster event (Problem Matrix shown above), the Help Desk will relate the problem to an appropriate BCP/DRP Recovery Plan (i.e., building 3 is on fire, or the police have told us to leave our building because of a Hazardous Materials release from a nearby company).
2. The BCP/DRP Recovery Plan will name the Contingency Recovery Coordinator and provide his contact information. The Help Desk operator will contact the Contingency Recovery Coordinator who will in turn start to call the Recovery Team Members listed in the BCP/DRP Recovery Plan.
3. A Situation Manager will coordinate recovery efforts being performed by the various Contingency Recovery Teams. These teams will be various areas within the company, and could also include vendors and clients as needed.

Testing and organizational acceptance

The purpose of DR/BC testing is to achieve organizational acceptance that the business continuity solution satisfies the organization's recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws, or solution implementation errors. Testing may include:

- Crisis command team call-out testing
- Technical swing test from primary to secondary work locations

- Technical swing test from secondary to primary work locations
- Application test
- Business process test

At minimum, testing is generally conducted on a biannual or annual schedule. Problems identified in the initial testing phase may be rolled up into the maintenance phase and retested during the next test cycle.

Maintenance

Maintenance of a BCP manual is broken down into three periodic activities. The first activity is the confirmation of information in the BCP manual and then a roll out to ALL staff for awareness and specific training for individuals whose roles are identified as critical in response and recovery. The second activity is the testing and verification of technical solutions established for recovery operations. The third activity is the testing and verification of documented organization recovery procedures. A biannual or annual maintenance cycle is typical, but some companies have decided to integrate BCP Plan / Manual maintenance within the Change Control process so that the BCP Manual is always current.

Information update and testing

All organizations change over time, therefore a BCP manual must change to stay relevant to the organization. Once data accuracy is verified, normally a call tree test is conducted to evaluate the notification plan's efficiency as well as the accuracy of the contact data. Some types of changes that should be identified and updated in the manual include:

- Staffing changes
- Staffing job function changes
- Changes to important clients and their contact details
- Changes to important vendors/suppliers and their contact details
- Departmental changes like new, closed or fundamentally changed departments.
- Changes in company investment portfolio and mission statement
- Changes in upstream/downstream supplier routes

Testing and verification of technical solutions

As a part of ongoing maintenance, any specialized technical deployments must be checked for functionality. Some checks include:

- Virus definition distribution
- Application security and service patch distribution
- Hardware operability check
- Application operability check

- Data verification

Testing and verification of organization recovery procedures

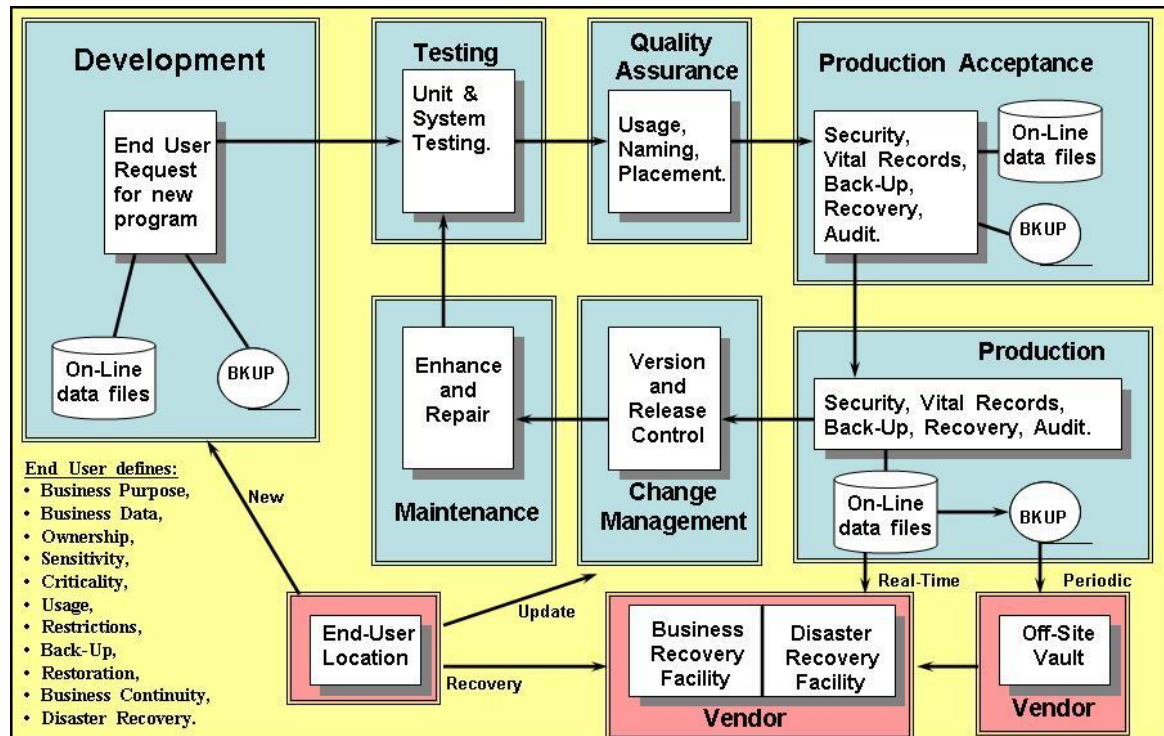
As work processes change over time, the previously documented organizational recovery procedures may no longer be suitable. Some checks include:

- Are all work processes for critical functions documented?
- Have the systems used in the execution of critical functions changed?
- Are the documented work checklists meaningful and accurate for staff?
- Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined Recovery Time Objective (RTO)?

Treatment of Test Failures

When establishing a BCP manual and recovery infrastructure from scratch, issues found during the testing phase often must be reintroduced to the analysis phase.

The Systems Development Life Cycle



Most organizations utilize a Systems Development Life Cycle like the one listed above. The activities performed during this SDLC include:

1. **Development** – the end user provides the information listed above along with the criticality of the application to be developed, the sensitivity of the application data, and the Recovery Time Objective needed to be achieved in order to recovery the application in accordance with its business needs.
2. **Testing** – confirms the applications operation and is performed on a modular and system level utilizing test data and validating the status of application operation. Usually, all error messages and application functions are included during Unit and System Testing.
3. **Quality Assurance** – confirms that application meets the standards and guidelines established by the organization and industry. Documentation is checked to verify that operations and support documents meet expectation. One of the documents included in this area could be a BCP/DRP Plan for the application.
4. **Production Acceptance** – is when the elements of an application are entered into the Production Libraries and naming conventions are verified. This housekeeping is needed to support applications in the Production environment and may include Data Sensitivity to support IT Information Security and Vital Records Management information to support Back-Up / Recovery operations.

5. **Production** – Is the environments where applications are processed on either mainframe computers or servers. This is the normal environment for applications.
6. **Change Management** – this environment is where applications reside when a problem or enhancement is requested. Decisions are made as to the best method for updating the application to repair a problem or implement an enhancement. Once approved for change, the application is sent to the Maintenance environment.
7. **Maintenance** – is where application updates are preformed in accordance to Change Management guidelines. After changes are made, the application will again go through the Testing, Quality Assurance, Production Acceptance, and Production cycles.

By following this sequence of events it is possible to maintain applications in the best condition needed to support business operations. Incorporating BCP/DRP Planning within the SDLC will allow for the integration of these two processes and reduce the effort needed to create and maintain BCP/DRP Plans.

Elements of the BCP/DRP Test Plan

How can you be sure your business continuity plans deal effectively with a wide range of potential disruptions or disasters? How can you be certain all the elements of your complex enterprise will recover using these plans or that they will stand up to an audit by the Regulator?

A comprehensive, multi-dimensional and on going BCP/DRP testing program is the only way to achieve the level of confidence you and your senior executives expect.

Our experts have: designed, managed and helped execute a testing program for many organizations comprised of the following elements:

- Assess your test experience and BCP / DRP objectives
- Recommend the type of tests that validate your enterprise's recovery objectives
- Design a long range testing program with clear, usable management metrics
- Prepare meaningful test scenarios, learning objectives, and success criteria
- Manage the staging and execution of scheduled tests
- Use command center tools to capture auditable, team actions, communication details, improvements and lessons learned during the test
- Develop pre and post test action plans to fill the gaps, prioritize organizational issues and plan improvements to your business continuity program.
- Recommend training and awareness curricula for test participants
- Review/Analyze the integration of plan maintenance and testing
- Develop training programs for future BCP test managers.

Business Continuity Plans can be progressively tested to confirm that maximum benefit is derived. The Methodology consists of the following phases:

Plan Audit

We will comment on the overall effectiveness of the plans and may suggest adjustments are made to the plans before any further test phases are commenced.

Passive Walk Through

This Phase will increase the awareness for all participants concerning their roles. Test Modules will be used to ensure a constant and structured approach.

Scenario Workshop

A Test Scenario is compiled based upon realistic circumstances to your industry / location and potential threats. The participants will be asked to invoke the plans and to perform their individual roles in order to recover from the scenario.

Physical Test

As a result of the Scenario Workshop, the Physical Test will involve the actual attendees at the recovery site and that recovery procedures are in order.

Live Simulation Test

As a result of the preceding phases, a live Simulation Test is the ultimate proof of the effectiveness of the plans. The Live Simulation Test should only be attempted when a high degree of confidence has been generated by the successful completion of the previous phases and consensus to the Live Test.

A Recovery Test Status Report will be produced at the end of each phase of the test with recommendations for improvement in the short, medium and long term provided with an ongoing maintenance program.

Forms used to Support BCP/DRP Implementation and Test Plans

In order to create and execute a BCP/DRP Test Plan it is necessary to utilize forms that make it easier for team members to follow a sequential scenario of events. There are four levels of BCP/DRP forms used to implement and test BCP/DRP plans, which are:

Level 1 - Executive Awareness and Authority

Level 2 - Plan development and documentation

Level 3 - Management & Recovery Team Assessment and Evaluation for Effectiveness

Level 4 - (Certification) Management & Recovery Team Assessment of Readiness and Plan Maintenance

Level 1 is used to provide high level management with a means to notify staff and management of the relative importance of the BCP/DRP effort and is used to authorize cooperation with the BCP/DRP teams. When performing BCP/DRP Testing, this level of authority is required to justify the efforts and costs associated Test Plan development and execution.

Level 2 is used to guide the Development and Implementation of BCP/DRP Plans. This form will help evaluate existing BCP/DRP plans that may be utilized during the Testing process.

Level 3 is used to assess how well management and staff have performed the functions needed to create, implement, and maintain BCP/DRP plans and Test Plans.

Level 4 is used to guide the creation of BCP/DRP Test Plans and to evaluate how well they were executed.

Level 1 - Executive Awareness and Authority

Level 2 - Plan development and documentation

Completed By:

Name: _____

Company: _____

Room: _____

Street: _____

City, State, Zip: _____

Phone Number: _____

Business Recovery _____

Plan for: _____

Business Recover Plan (BRP.--LEVEL 1 (Executive Awareness/Authority.	Y	N	N/A
1. Has a BRP been: <ul style="list-style-type: none"> a. Developed? b. Updated within the last 6 months? 			
Business Recover Plan (BRP.--LEVEL 2 (Plan Development and Documentation.	Y	N	N/A
1. Has a classification (critical, important, marginal) been assigned to the Business Process/Function/ Component that this Facility/Function supports?			
2. Has a BRP been: <ul style="list-style-type: none"> a. Documented? b. Maintained? 			
3. Does the BRP include the following sections: <ul style="list-style-type: none"> a. Identification? b. Incident Management? <ul style="list-style-type: none"> i. Responsible company officer? ii. Personnel responsible for updates? c. Response? d. Recovery? e. Restoration? f. Plan Exercise? g. Plan Maintenance? h. Business Recovery Teams and Contact Information? 			

4. Does the BRP identify hardware and software critical to recover the Business and/or Functions?			
5. Does the BRP identify necessary support equipment (forms, spare parts, office equipment, etc.) to recover the Business and/or Functions?			
6. Does the BRP require an alternate site for recovery? a. Does the BRP provide for mail service to be forwarded to the alternate facility? b. Does the BRP provide for other vital support functions?			
7. Are all critical or important data required to support the business being backed up? a. Are they being stored in a protected location (offsite)?			
8. Do you conduct a walk-through exercise of your Plan at least annually? (This should include a full walk-through as well as "elements" of your plan (i.e. accounts payable, receivable, shipping and receiving, etc).			
9. Does the walk-through element exercises have a prepared plan which includes: a. Description b. Scope c. Objective			
10. Is a current copy of the BRP maintained off-site?			
11. Do all users of the BRP have ready access to a current copy at all times?			
12. Is there an audit trail of the changes made to the BRP?			
13. Do all employees responsible for the execution of the BCP/DRP receive ongoing training in Disaster Recovery and Emergency Management?			

Level 3 - Management & Recovery Team Assessment and Evaluation for Effectiveness

Business Recover Plan (BRP)--LEVEL 3 (Management & Recovery Team Assessment and Evaluation For Effectiveness)	Y	N	N/A
1. Has the business officer and management team approved the BRP?			
2. Does the business owner maintain: <ul style="list-style-type: none"> a. The master copy of the BRP? b. An audit trail of the changes made to a BRP? 			
3. Do all aspects of physical and logical security at the alternate site conform to your current security procedures?			
4. Are the physical and logical security procedures at the alternate site at least as stringent as the security at the disaster location?			
5. Have all employees and their alternates responsible for executing a manual work-around for a mechanized process been identified in the BRP and properly trained?			
6. Has an independent observer documented the simulation exercise(s) noting all results, discrepancies, exposures, action items, and individual responsible, etc.?			
7. Was a debriefing held within a reasonable period of time (typically two weeks) after the simulation exercise(s) to ensure all activities have been accurately recorded?			
8. Did the exercise coordinator publish a simulation exercise(s) report within a reasonable period of time (typically three weeks) after the completion of the simulation exercise(s)?			
9. Did the exercise report include: <ul style="list-style-type: none"> a. What worked properly as well as any deficiencies and recommendations for improvement? b. Responsibility and due date for the development of the Corrective Action Plan? 			
10. Was a Corrective Action Plan developed by the Exercise Team to address any deficiencies identified by the exercise?			

<p>11. Is there a retention plan for the Exercise Plans and Corrective Action Plans (minimum retention 3 years)?</p>			
<p>12. Has a walk-through element exercise been performed at least quarterly?</p>			
<p>13. Did each walk-through element exercise have a prepared plan which includes: a) Description b) Scope c) Objective</p>			
<p>14. When there is a change in hardware, software, or a process that might impact the Business Recovery Plan, is the BRP reviewed and updated within 30 days of the changes: Sign-Off By Officer: by whom? Name: _____ When? Date: _____</p>			
<p>15. Based on the Joint Assessment has the Team determined that the BRP is effective?</p>			

Level 4 - (Certification) Management & Recovery Team Assessment of Readiness and Plan Maintenance

Business Recover Plan (BRP)--LEVEL 4 (Certification) (Management & Recovery Team Assessment Of Readiness and Plan Maintenance)	Y	N	N/A
1. Has the component BRP been approved by the owner(s) of the Business Function(s)?			
2. Has the entire BRP simulation exercise been performed at least annually?			
3. Has the Corrective Action Plan been completed and closed?			
4. Did the BRP simulation exercise have a prepared plan which includes: a. Description b. Scope c. Objective			
5. Did the component BRP simulation exercise meet the acceptable Recovery Time Objective set by management?			
6. Based on the Joint Assessment has the Team determined that the BRP and Exercises have met all requirements to provide reasonable assurance that the plan will work in the event of a disaster?			
7. Does the BRP specify the maximum acceptable Recovery Time Objective (RTO)?			
8. Does the BRP specify the level of service (which the business owner has agreed to be acceptable) to be provided while in recovery mode?			
9. Have all changes relating to RTO in the BRP been approved by the process owner?			